INSTITUTO DE ESTUDOS SUPERIORES MILITARES
CURSO DE ESTADO-MAIOR CONJUNTO

2014 / 2015

TII

A UTILIZAÇÃO DAS REDES SOCIAIS POR ELEMENTOS MILITARES: O USO SIMULTÂNEO EM AMBIENTES DE TRABALHO NO ÂMBITO DA DEFESA

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

A UTILIZAÇÃO DAS REDES SOCIAIS POR ELEMENTOS MILITARES: O USO SIMULTÂNEO EM AMBIENTES DE TRABALHO NO ÂMBITO DA DEFESA

MAJ TM Paulo Jorge da Silva Carvalho

Trabalho de Investigação Individual do CEMC 2014/15

Pedrouços 2015

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

A UTILIZAÇÃO DAS REDES SOCIAIS POR ELEMENTOS MILITARES: O USO SIMULTÂNEO EM AMBIENTES DE TRABALHO NO ÂMBITO DA DEFESA

MAJ TM Paulo Jorge da Silva Carvalho

Trabalho de Investigação Individual do CEMC 2014/15

Orientador: CTen M João José Laranjeira de Brito Afonso

Pedrouços 2015

Agradecimentos

Durante a realização deste trabalho de investigação individual beneficiei da confiança e do apoio de algumas pessoas para com as quais sinto uma enorme gratidão e aqui expresso o meu reconhecimento.

Ao meu orientador, CTen Brito Afonso, agradeço o entusiasmo com que sempre abordou este tema, as suas críticas e sugestões, e a sua permanente disponibilidade para me receber.

Ao Sr. Major Paulo Mineiro, Chefe da Área de Informação Pública da Força Aérea Portuguesa, agradeço a sua disponibilidade para a realização da entrevista que constituiu um valioso contributo para que este trabalho refletisse uma visão mais completa da realidade portuguesa, só possível com a partilha dos seus conhecimentos e experiência.

À Marktest, agradeço profundamente a gentileza da cedência para fins académicos dos dados do seu estudo “Os portugueses e as Redes Sociais 2014”, constituindo estes um valioso contributo para atingir o objetivo geral do meu trabalho.

Aos meus camaradas de curso também o agradecimento pelo seu companheirismo e pelo entusiasmo com que me contagiaram no cumprimento das muitas tarefas do curso.

À minha família o agradecimento especial pelo seu apoio incondicional e pela resiliência com que lidou com a minha ausência num período de trabalho intenso.

Índice

Introdução 1

a. Introdução ao tema e definição do contexto da investigação 1
b. Justificação e importância da investigação 2
c. Objeto de estudo e sua delimitação 4
d. Definição dos objetivos da investigação 4
e. Percurso metodológico 4
f. Organização do estudo 6

1. O que são as redes sociais 7

a. Enquadramento temporal e espacial 7
b. A esfera de presença: individual ou organizacional 13
c. Os riscos da utilização das redes sociais 15
d. Os hábitos dos portugueses nas redes sociais 18
e. Síntese conclusiva 22

2. A utilização das redes sociais por elementos militares 23

a. A importância das Relações Públicas na defesa 23
b. A importância da Segurança da Informação na defesa 24
c. A busca de um compromisso na utilização das redes sociais pelos militares 26
d. Caso de estudo: a política de utilização das redes sociais norte-americana 28
e. Síntese conclusiva 31

3. A conceção de uma política comum de utilização das redes sociais 32

a. A realidade da defesa em Portugal 32
b. A criação de uma *framework* para a política de utilização 34
c. A definição de uma política de monitorização organizacional 39
d. A utilidade da criação de uma rede social própria da defesa 41
e. Síntese conclusiva 42

Conclusões e recomendações 43

a. Conclusões 43
b. Recomendações 45

Índice de Anexos

Anexo A – Investigação quantitativa relativa à utilização das redes sociais pelos portugueses.....Omitido
Anexo B – Princípios orientadores para a política de utilização das RS pelos militares da defesa..... Anx B-1
Anexo C – Processo interno do *Department of Defense* dos EUA para revisão da informação a publicar nas RS ..... Anx C-1
Anexo D – Técnicas recomendadas pelo Exército dos EUA para a construção de páginas no Facebook ..... Anx D-1
Anexo E – Técnicas recomendadas pelo Exército dos EUA para a utilização do Twitter ..... Anx E-1
Anexo F – Dicas de segurança recomendadas pelo Facebook no seu Guia de Segurança .....Anx F-1

Índice de Apêndices

Apêndice A – Modelo de análise..... Apd A-1
Apêndice B – Guião da entrevista realizada ao Chefe da Área de Informação Pública da Força Aérea Portuguesa em 27/3/2015 ..... Apd B-1

Índice de Figuras

Figura 1 - *Post* dos militares da Wisconsin National Guard no Instagram 3
Figura 2 - Fases e respetivos passos da investigação 5
Figura 3 - Captura de ecrã do sítio da Rede Social Friendster 8
Figura 4 - Página de entrada do sítio da Rede Social MySpace 10
Figura 5 – Perfil no Facebook de Mark Zuckerberg, seu fundador e CEO desde 2004..... 12
Figura 6 - Top 15 dos sítios mais populares de redes sociais em março de 2015 13
Figura 7 - Perfil no Facebook da Robin Sage, após ter sido desmascarado 17
Figura 8 - Redes sociais onde os portugueses estavam presentes em 2014 20
Figura 9 – Funcionalidades que os portugueses utilizavam nas redes sociais em 2014..... 21
Figura 10 – Períodos horários em que os portugueses acediam às redes sociais em 2014 . 21
Figura 11 – Tempo de permanência dos portugueses nas redes sociais em 2014 22
Figura 12 – Frequência de visita dos portugueses às redes sociais em 2014 22
Figura 13 – Pessoal militar, segundo regime e situação, em 31 de dezembro de 2012..... 27

Figura 14 - Militares do QP no ativo, quanto à efetividade de serviço 28
Figura 15 - Diretório das presenças oficiais do Exército dos EUA em sítios públicos dos *media* sociais 30
Figura 16 – Sítio da Defesa Nacional na Internet..... 33
Figura 17 – Sítio da Marinha portuguesa na Internet 33
Figura 18 - Sítio da Força Aérea portuguesa na Internet..... 33
Figura 19 - Ficheiro que define as áreas do sítio do Facebook que podem ser acedidas por um *crawler* 40
Figura 20 - Fluxograma do processo interno de revisão da informação do *DoD*..... Anx B-1

Índice de Tabelas

Tabela 1 - Ranking do número de utilizadores da Internet, por país, em 2014..... 19
Tabela 2 - Ranking da taxa de penetração da Internet, por país, em 2014..... 19
Tabela 3 - Universo e Amostra do estudo ..... Omitida
Tabela 4 - Redes Sociais onde tem perfil criado ou possui conta ..... Omitida
Tabela 5 - Funcionalidades das Redes Sociais que costuma utilizar..... Omitida
Tabela 6 - Períodos horários de acesso a sítios de Redes Sociais ..... Omitida
Tabela 7- Em média, por dia, quanto tempo costuma dedicar aos sítios de Redes Sociais ..... Omitida
Tabela 8 - Frequência de visita aos sítios de Redes Sociais – Total ..... Omitida
Tabela 9 - É fã de empresas/marcas nas Redes Sociais..... Omitida
Tabela 10 - Conceitos, Dimensões e Indicadores associados à Hipótese 1..... Apd A-1
Tabela 11 - Conceitos, Dimensões e Indicadores associados à Hipótese 2..... Apd A-1
Tabela 12 - Conceitos, Dimensões e Indicadores associados à Hipótese 3..... Apd A-2

Resumo

Até ao momento não foi definida pela Defesa Nacional uma política de utilização das redes sociais por elementos militares nos ambientes de trabalho.

Como tal, cada uma das organizações que a integram tomam decisões autónomas no estabelecimento de regras aplicáveis a esta matéria e desvalorizam o papel que a formação pode ter na preparação dos militares para minimizar os problemas de segurança que estes podem criar quando as utilizam. Ainda que não intencionais, estes problemas podem comprometer a segurança da informação ou das operações, ou mesmo prejudicar a reputação dessas organizações.

Sendo desejável a criação desta política, é necessário compreender as redes sociais e estudar os hábitos dos militares enquanto utilizadores, para que com este conhecimento seja possível propor uma *framework* para a sua implementação eficaz, composta por um conjunto de regras de acesso, de normas de conduta e dum plano de formação, aplicáveis aos militares utilizadores das redes sociais.

Palavras-chave

Redes Sociais, INFOSEC, OPSEC, Política de Utilização, Normas de Conduta.

Abstract

So far it hasn't been defined by the National Defence a policy for the use of social networks by military personnel in the workplace.

As such, each of its member organizations take autonomous decisions in the establishment of rules applicable to this matter and devalue the role that education can play in preparing the military to minimize the security problems they can create when using them. Although unintentional, these problems can compromise the security of information or operations, or even damage the reputation of these organizations.

For the creation of such desirable policy, it is necessary to understand social networks and study the habits of the military as their users, so that with this knowledge it is possible to propose a framework for its effective implementation, consisting of a set of access rules, standards of conduct and a training plan, applicable to the military personnel who are social networks users.

Keywords

Social Networks, INFOSEC, OPSEC, Policy of Use, Standards of Conduct.

Lista de abreviaturas, siglas e acrónimos

D	
DoD	*Department of Defense*
E	
EEFI	Elementos Essenciais de Informação Amiga
EMFAR	Estatuto dos Militares da Forças Armadas
EUA	Estados Unidos da América
F	
FA	Força Aérea
FBI	*Federal Bureau of Investigation*
FFAA	Forças Armadas
H	
H	Hipóteses
I	
INFOSEC	Segurança das Informações
N	
NSA	*National Security Agency*
O	
OTAN	Organização do Tratado do Atlântico Norte
OPSEC	Segurança das Operações
P	
PAO	Oficial de Relações Públicas
PDE	Publicação Doutrinária do Exército
Q	
QC	Questão Central
QD	Questões Derivadas
R	
RDM	Regulamento de Disciplina Militar
RP	Relações Públicas
RS	redes sociais

T

TII	Trabalho de Investigação Individual

U

URL	*Uniform Resource Locator*

V

VUD	visitantes únicos diários

Introdução

a. Introdução ao tema e definição do contexto da investigação

O presente Trabalho de Investigação Individual (TII) insere-se no âmbito da unidade curricular Trabalho Final de Curso do plano curricular do Curso de Estado-maior Conjunto 2014-15, e pretende abordar a temática da utilização das redes sociais (RS) em ambientes de trabalho no âmbito da defesa, sobretudo marcados por requisitos de segurança muito exigentes.

As RS são um fenómeno moderno cuja popularidade tem crescido ao mesmo ritmo a que novos utilizadores se têm ligado à Internet. Este crescimento deve-se sobretudo ao facto destas redes estarem muito centradas nos utilizadores e lhes permitirem fazer uso da tecnologia para criarem laços sociais, dos quais dependem por essência. Para além disso, muitos outros sítios na Internet reconheceram a importância destas redes e adotaram funcionalidades de ligação aos seus próprios conteúdos, que vieram reforçar ainda mais a sua utilidade (Mislove, 2009).

Consequentemente, o alcance e o sucesso que estas redes obtiveram levaram a que também as organizações e as empresas se envolvessem nas mesmas, uma vez que a expressão deste fenómeno potenciava a influência em massa de indivíduos. Através do Marketing esta potenciava a criação de novos mercados e através das Relações Públicas (RP) potenciava a construção ou reforço de uma imagem positiva, aumentando a sua notoriedade ou credibilidade.

No entanto, a sua utilização trouxe todo um conjunto de vantagens mas expôs simultaneamente os seus utilizadores a riscos indesejados, nomeadamente a perseguição emocional, o roubo de identidade ou até a exploração de informação pessoal para a criação de oportunidades de ataque físico. Tal como os utilizadores, as organizações acabaram por se expor aos mesmos riscos já que, sendo ténue a fronteira que separa os conteúdos puramente pessoais dos conteúdos relacionados com a atividade profissional, os utilizadores acabaram por envolvê-las de forma indireta, dificultando-lhes ou impedindo-lhes o controlo dos potenciais efeitos desse envolvimento.

O setor de atividade da defesa, em particular, caracteriza-se por tornar as suas organizações sensíveis em termos de segurança muito nomeadamente no que diz respeito à Segurança da Informação, e o papel que os seus colaboradores, sejam este militares ou civis, podem ter na revelação de matérias sensíveis ou confidenciais, ainda que o fazendo na maior parte das vezes de forma inconsciente, constitui a principal ameaça.

Pela sua natureza as RS constituem um território perigoso para a ocorrência destes problemas, mas não sendo desejável ou até possível que uma empresa ou organização possa proibir o seu uso aos seus colaboradores, já que este constitui em parte um direito fundamental da esfera da vida privada das pessoas, resta-lhes conceber um plano de proteção e persuadir os seus colaboradores a fazerem parte dele. A conceção de tal plano nasce do cálculo dos riscos e das oportunidades, procurando posteriormente minimizar os primeiros e maximizar as segundas.

b. Justificação e importância da investigação

A defesa em Portugal não definiu até ao momento uma política comum para a utilização das RS, aplicável a todas as entidades ou organizações sob a sua tutela, o que deixa espaço para decisões autónomas dos diferentes decisores no estabelecimento de regras aplicáveis a esta matéria podendo daqui resultar em alguns casos, uma utilização perigosamente desregulada.

Países como os Estados Unidos da América (EUA), o Reino Unido ou a Austrália, constituem boas referências por terem estudado profundamente os hábitos dos seus utilizadores nas RS e terem definido políticas oficiais para a utilização das RS na defesa, comuns ou não às diferentes organizações que a integram, complementadas pela criação simultânea de um conjunto de normas de conduta para os utilizadores e um plano de formação para a sua aplicação envolvendo não apenas os seus colaboradores mas também os seus familiares.

O caso dos EUA tornou-se mesmo a referência para todo o mundo em matéria desta regulação, quando em 2010 definiu oficialmente uma política comum para a utilização das RS na defesa, sendo um dos primeiros países a autorizar as suas organizações a possuir uma presença oficial nas RS e a autorizar os seus colaboradores a aceder às RS nos próprios computadores da defesa. As principais motivações para o fazer relacionavam-se com a grande comunidade de utilizadores militares e com a forte atividade da defesa dos EUA à escala global, que obriga os militares a procurar meios de comunicação que lhes permitam ultrapassar as grandes distâncias e os longos períodos que os separam das suas famílias.

Contudo, escândalos recentes com origem numa má utilização das RS têm causado embaraço à defesa norte-americana e reavivaram a argumentação dos que se opunham à permissão de utilização das RS, vindo demonstrar que as políticas são definidas de acordo com uma determinada conjuntura mas poderão ter de ser revistas, caso, e quando, as

circunstâncias se alterem. A simples existência de normas de conduta para a utilização das RS não é por si suficiente, pois os seus efeitos dependem do grau de sucesso da sua aplicação. Senão veja-se a título de exemplo na Figura 1, o efeito de consternação que uma fotografia publicada nas RS por militares pertencentes a uma unidade que lida com o repatriamento de militares americanos mortos em combate pode causar, ao evidenciar um tom de celebração em algo tão solene quanto a guarda do caixão de um jovem, cuja vida foi perdida ao serviço da pátria.

Figura 1 - *Post* dos militares da Wisconsin National Guard no Instagram

Fonte: http://www.stripes.com/news/us/2nd-national-guard-soldier-suspended-over-casket-photo-scandal-1.268619

Este trabalho irá focar-se nos hábitos dos utilizadores das RS públicas para compreender os riscos inerentes à sua utilização por parte dos militares das Forças Armadas (FFAA) portuguesas em ambientes de trabalho da defesa, considerando que:

-o problema antigo da fuga de informação, anteriormente associado ao boca a boca transitou para a Internet e particularmente para as RS, por nestas ter encontrado uma forma de chegar mais rápido e a um número infinitamente maior de pessoas num ambiente muito informal, onde o propósito é a partilha de informação;

-e que o caso particular do setor da defesa apresenta algumas limitações ao seu uso pleno dadas as características próprias que tornam este uso mais sensível a questões de perda de confidencialidade ou até de adoção de condutas pessoais inapropriadas.

c. Objeto de estudo e sua delimitação

O objeto da investigação são os militares das FFAA portuguesas, mas será delimitado aos que estando na efetividade de serviço sejam utilizadores das RS em ambientes de trabalho no âmbito da defesa.

d. Definição dos objetivos da investigação

(1) Objetivo geral

O objetivo geral da investigação é avaliar as vantagens e desvantagens da existência de uma política comum para a utilização simultânea das RS em ambientes de trabalho no âmbito da defesa e avaliar a utilidade da criação de uma rede social interna.

(2) Objetivos específicos

(a) Analisar as questões associadas à Segurança da Informação;

(b) Identificar uma *framework* de elaboração de uma política comum de utilização das RS que salvaguarde a segurança da informação, a segurança das operações e que evite a adoção de condutas pessoais inapropriadas por parte dos militares;

(c) Analisar os aspetos relevantes do uso de uma rede social própria da defesa para uso interno.

e. Percurso metodológico

Este trabalho de investigação foi desenvolvido com recurso ao método científico e a investigação foi direcionada ao longo duma linha conducente à obtenção de uma reposta, tão clara e completa quanto possível, para a seguinte **Questão Central (QC)**:

QC - Em que medida as Forças Armadas devem permitir e regular o uso das RS em ambientes de trabalho no âmbito da defesa?

O tipo de raciocínio utilizado foi o hipotético-dedutivo, começando-se por formular as hipóteses ou teorias que irão condicionar as observações a efetuar no decurso da investigação para verificar a sua veracidade.

No sentido de operacionalizar a formulação destas hipóteses foram ainda formuladas três **Questões Derivadas (QD)**:

QD1 – Como são hoje as RS e qual a relação dos portugueses com estas enquanto seus utilizadores particulares ou profissionais?

QD2 – A especificidade das atividades desenvolvidas pela defesa impede o uso das RS nos seus ambientes de trabalho?

QD3 - É possível criar regras que minimizem as ameaças e tornem aceitável o uso simultâneo das RS por elementos militares?

A partir destas QD levantaram-se as seguintes **Hipóteses (H)** orientadoras do estudo:

H1 – As RS são um fenómeno em contínuo crescimento, com características distintas em termos geográficos e dinâmicas imprevisíveis, e são para os portugueses que acedem regularmente à Internet algo indispensável.

H2 - A tecnologia está cada vez mais presente nos ambientes de trabalho da defesa e o uso das RS em simultâneo nestes ambientes aumenta fortemente a ameaça à segurança da informação e à segurança das operações.

H3 - É necessário criar normas de conduta para os militares que utilizam as RS e as semelhanças existentes nas diversas estruturas das FFAA aconselham a definição de uma política comum.

O procedimento metodológico seguido foi o definido na publicação intitulada "Orientações Metodológicas para a Elaboração de Trabalhos de Investigação" do IESM, (Santos, et al., 2014). As três fases previstas neste procedimento (a exploratória, a analítica e a conclusiva) percorreram os passos representados na Figura 2.

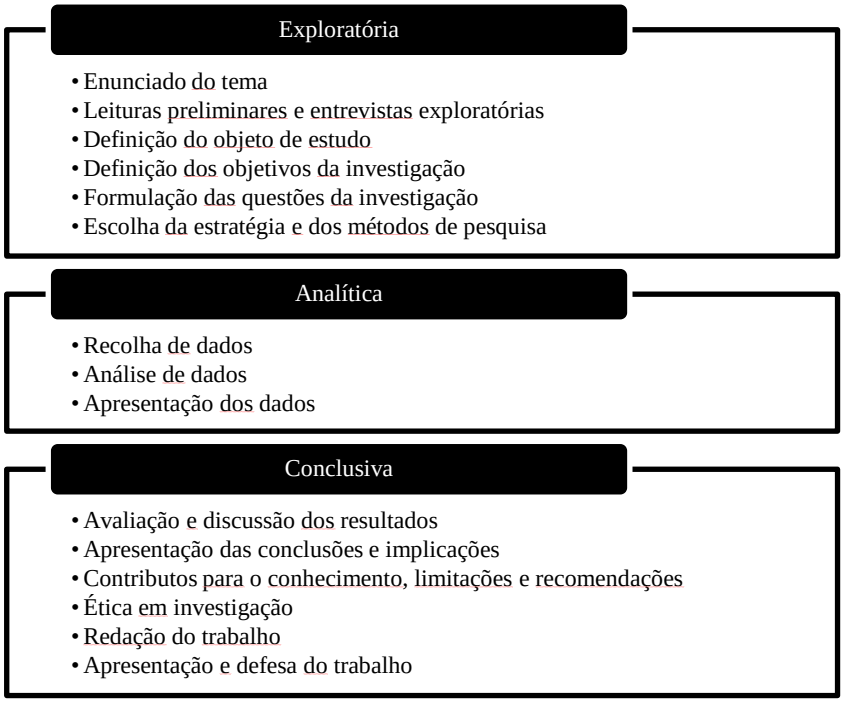

Figura 2 - Fases e respetivos passos da investigação
Fonte: (Santos, et al., 2014, pp. vi-vii)

A estratégia da investigação será mista incorporando elementos de origem qualitativa e quantitativa, e a sua recolha foi direcionada através do modelo conceptual descrito no

Apêndice A. Os instrumentos de observação utilizados para a recolha de dados de origem qualitativa foram a análise documental de documentos e legislação enquadrantes, e a realização de uma entrevista (Apêndice B) ao Chefe da Área da Informação Pública da Força Aérea portuguesa. Os dados de origem quantitativa foram extraídos do estudo realizado anualmente pela Marktest Consulting, intitulado "Os Portugueses e as Redes Sociais 2014", dados esses que foram gentilmente cedidos para a realização deste trabalho académico, na condição de não poderem ser utilizados para qualquer outro efeito. O instrumento de observação utilizado na recolha destes dados foram entrevistas *online* (Cawi[1] System), tendo por base um questionário estruturado de autopreenchimento, constituído por perguntas fechadas e abertas que decorreram entre os dias 3 e 29 de Setembro de 2014 (Anexo A). Este estudo tem o objetivo de conhecer índices de notoriedade, utilização, opinião e hábitos dos portugueses face às RS. Para tal, procurou conhecer os hábitos dos utilizadores de RS, os sítios que conhecem e mais utilizam, as funcionalidades que mais valorizam, a frequência com que acedem aos sítios e com que neles publicam informação, assim como o tempo que lhes dedicam ou os equipamentos que utilizam para lhes aceder. Esta informação permitiu avaliar os aspetos a considerar na definição de uma política comum de utilização das RS para a defesa, que seja a mais indicada para ser aplicada aos militares nos seus ambientes de trabalho.

A referenciação bibliográfica foi efetuada utilizando o *software* Microsoft Word 2007, tendo sido adotado o estilo Harvard-Anglia.

f. Organização do estudo

O trabalho está organizado em três capítulos, introdução e conclusão. Na introdução efetua-se a contextualização e justificação do tema, e enunciam-se os objetivos e o percurso metodológico da investigação. O primeiro capítulo trata a história das RS, a sua compreensão e os hábitos dos seus utilizadores. O segundo capítulo trata as vantagens e desvantagens da utilização das RS no contexto da defesa e analisa o caso de estudo da defesa dos EUA. O terceiro capítulo trata a criação de uma política comum de utilização das RS para a defesa nacional, propondo uma *framework* composta por um conjunto de regras de acesso, de normas de conduta e dum plano de formação, e trata ainda de avaliar a pertinência da criação de uma RS própria da defesa. Na conclusão apresenta-se o entendimento das deduções extraídas da investigação e responde-se à questão central.

[1] *Computer-assisted web interviewing*.

1. O que são as redes sociais

a. Enquadramento temporal e espacial

O conceito de Rede Social foi definido por Boyd e Ellison (2007, p. 2) como um serviço *online* que permite aos indivíduos:

-construir um perfil público ou semipúblico no seio de um sistema fechado;

-dispor de uma lista de outros utilizadores com os quais partilham uma ligação;

-e explorar a sua própria lista de contatos bem como as listas de contatos dos outros.

A terminologia "social" presente neste conceito refere-se às necessidades instintivas que os seres humanos têm de estabelecer uma ligação com outros seres humanos. Existe em nós a necessidade inata de estar incluídos em grupos e estar rodeados de pessoas que sejam semelhantes a nós, que pensem como nós e com as quais nos sintamos confortáveis ao partilhar os nossos pensamentos, ideias e experiências. Desde que a nossa espécie começou que temos vindo a estabelecer estas ligações, mas, ao longo do tempo temos inventado novas formas de fazer. O termo *media* sociais, ou *social media* em inglês, refere-se aos meios e aos conteúdos de comunicação que usamos para estabelecer essas conexões com os outros seres humanos. Já usámos para fazer essas conexões tambores, fumos, o telégrafo, o telefone, o rádio, a televisão, o telemóvel, mas mais recentemente usamos o computador e o *smartphone*. O conteúdo da comunicação também evoluiu da fala para a escrita, e agora para formas mais complexas que combinam mensagens de texto, áudio, imagem e vídeo (Safko, 2012, p. 4).

Mas ironicamente o percurso histórico das RS teve na sua origem um grupo de pessoas isolacionistas que passavam os seus dias sentados à frente de um teclado de computador sem qualquer ligação ao exterior, conhecidos vulgarmente por *nerds* ou *geeks*, e que representavam o estereotipo de pessoas verdadeiramente antissociais. Foram estas pessoas que lideraram os primeiros passos dados para criar os primeiros espaços de encontro *online* que se designavam *Bulletin Board System*, ou BBS, na altura em que se começavam a desenvolver meios de comunicação capazes de interligar os computadores em rede fora do mesmo local, e que depois evoluiu para aquilo que todos nós conhecemos como Internet, ou como a rede de redes[2]. Tratava-se de uma ligação dos utilizadores a um sistema central a partir do qual podiam carregar ou descarregar ficheiros, na maior parte das vezes tratando-se de *software* pirateado, e onde também podiam deixar as suas mensagens para outros utilizadores a fim de partilharem os seus projetos e o seu

[2] Tal como definido pelo RFC1122 dos Internet Standard (Internet Engineering Task Force, 1989).

conhecimento. Apesar das grandes restrições impostas pela tecnologia de então a estes sistemas, sobretudo devido às ligações serem através de linha telefónica e se caracterizarem por ter velocidades de ligação extremamente baixas, estes tiveram grande sucesso e a sua longevidade espalhou-se pelas décadas de 1980 e 1990 (Digital Trends Staff, 2014).

Mas foi preciso esperar até 1997 para que surgisse o primeiro sítio da Internet que se encaixava na definição de RS apresentada anteriormente, chamado SixDegree.com (por causa da teoria com o mesmo nome que defende que todas as pessoas do mundo podem ser interligadas apenas por seis graus de separação) e que oferecia as duas componentes essenciais de uma RS que eram a criação de perfis dos utilizadores, e a criação de uma lista de perfis que consideravam "Amigos" e pelos quais podiam navegar (Boyd & Ellison, 2007, p. 4).

Depois deste, seguiram-se ainda três casos notáveis que por terem constituído verdadeiros marcos na história das RS não podem deixar de ser analisados: o Friendster, o MySpace e o Facebook.

O Friendster foi lançado em 2002 com o intuito de ser um sítio que ajudava as pessoas a conhecer-se, com a esperança de virem a ter uma relação, mas diferenciando-se de outros sítios semelhantes por não explorem a aproximação de pessoas completamente desconhecidas mas sim, a aproximação entre "amigos dos amigos" (Figura 3), os quais se acreditava serem melhores parceiros românticos do que os estranhos.

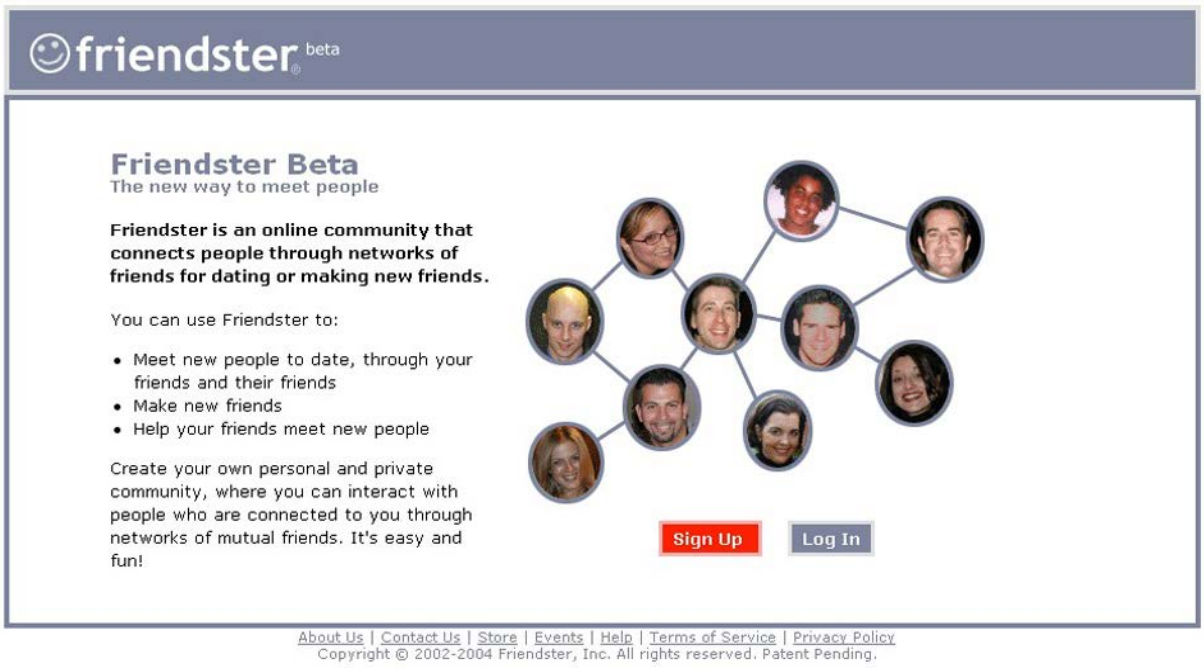

Figura 3 - Captura de ecrã do sítio da Rede Social Friendster
Fonte: http://www.digitaltrends.com/features/the-history-of-social-networking/

O facto de ter conseguido alcançar rapidamente 300.000 utilizadores levou a que a comunicação social lhe desse muita atenção, e o resultado imediato foi um aumento exponencial da sua popularidade, de tal forma que confrontou a infraestrutura de suporte do sítio com problemas de capacidade para acompanhar um número tão elevado de acessos. Outros problemas inovadores surgiram também na gestão dos utilizadores, obrigando mesmo à tomada de decisão dos administradores do Friendster de eliminar alguns perfis, os quais revelaram ser falsos, e procuravam por exemplo simular celebridades para atrair um maior número de amigos, ou sendo de utilizadores verdadeiros utilizavam fotografias de perfil que não eram suas. Por outro lado, a fama que alcançou como RS contribuiu para que nos finais de 2003 começassem a surgir dezenas de outras, muitas delas inspiradas no seu formato, o que, conjugado com os problemas referidos anteriormente lhe roubou a sua notoriedade (Boyd & Ellison, 2007, pp. 6-7).

O MySpace nasce precisamente nesse período, e no meio de tantas outras não despertou no início muita atenção. No entanto, nessa sua fase de arranque beneficiou de rumores que davam conta de que o Friendster se preparava para cobrar pela utilização do seu sistema, e do feliz acaso de um conjunto de bandas musicais o ter escolhido para estarem presentes nas RS e terem conseguido "arrastar" consigo os seus fãs que também aderiram em massa. Era uma relação mutuamente benéfica que se estabelecia entre ambos já que as bandas conseguiam uma forma eficaz de comunicar com os fãs e estes ali sentiam que tinham a atenção das bandas.

Dois fatores de sucesso do MySpace foram a capacidade de se ajustar às necessidades dos utilizadores, adicionando com regularidade funcionalidades que estes sugeriam, e a capacidade de permitir aos utilizadores personalizarem as suas próprias páginas, através de blocos de código html[3] que podiam facilmente ser partilhados entre utilizadores através de uma ação de copiar/colar, resultando em páginas verdadeiramente únicas com diferentes combinações de fundos e arranjos. Outro aspeto fundamental terá sido a resposta dada pelo MySpace à adesão em massa, verificada em 2004, por parte de adolescentes, atraídos não apenas pela presença das bandas mas também pela influência doutros elementos mais velhos das suas famílias. Em vez de rejeitar a presença de utilizadores menores de idade o MySpace alterou a sua política a fim de a permitir. Depois de os primeiros se conseguirem registar foram eles próprios a encorajar os seus amigos a

[3]Html,, ou *Hypertext Markup Language*, é uma linguagem para descrever a estrutura das páginas de Internet (W3C, 2015).

fazê-lo também. O seu grande sucesso levou a que a News Corporation o adquirisse por 580 milhões de dólares o que atraiu todas as atenções dos *media* a nível mundial. O sucesso cresceu de tal forma que se começou a tornar um fenómeno global, o qual só veio a abrandar quando posteriormente despontaram uma série de questões relacionadas com segurança, que implicavam este sítio como facilitador de relações entre adultos e menores, e que conseguiu provocar o pânico moral relativo à existência de predadores sexuais nas RS (Boyd & Ellison, 2007, pp. 8-9).

Depois de ter sido considerado a RS mais proeminente a nível mundial, sofreu uma tamanha perda de popularidade que levou este sítio inclusive, em 2010, a tentar reinventar-se através de uma renovação total que fazia nascer um novo "MySpace". Para além de um aspeto gráfico totalmente renovado (Figura 4) o sítio afirmava querer agora ser "o líder dos destinos de entretenimento" alimentando "a paixão de fãs de todo o mundo" (Parr, 2010), mas, como veremos mais à frente a sua ambição não passou disso mesmo e este não se encontra entre as RS mais populares na atualidade.

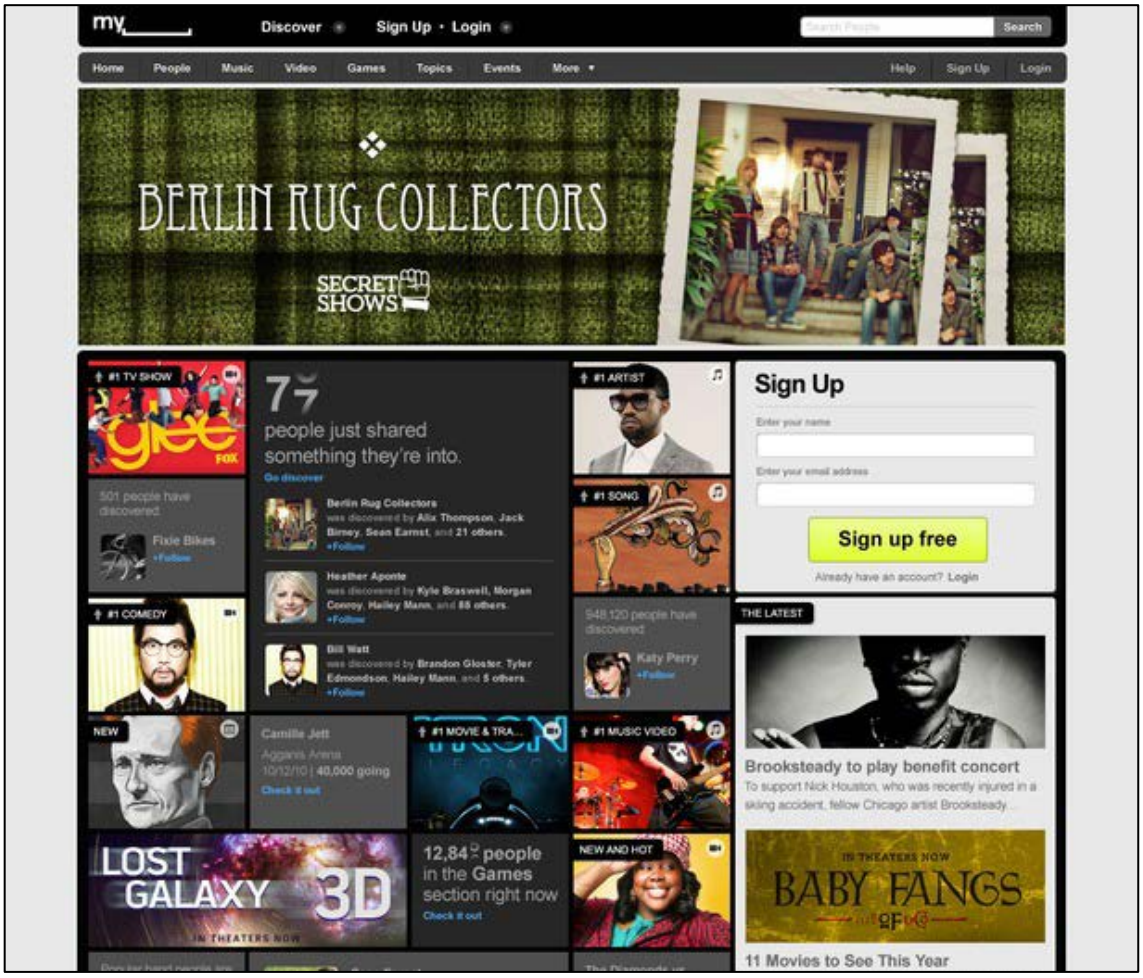

Figura 4 - Página de entrada do sítio da Rede Social MySpace
Fonte: http://mashable.com/2010/10/26/new-myspace/

Ainda no início de 2004, Mark Zuckerberg (Figura 5) e outros quatro colegas de universidade criaram outra RS chamada Facebook a qual apresentava uma característica muito distinta das anteriores. Esta tinha que ver com uma limitação do universo de utilizadores a uma comunidade fechada, que naquele caso correspondia à comunidade formada exclusivamente pelos utilizadores da rede informática da Universidade de Harvard, que para aderirem àquela RS precisavam ter um endereço de correio eletrónico associado àquela instituição. O sucesso que alcançou fez com que naturalmente se expandisse, primeiro a outras universidades, e posteriormente às escolas secundárias e às empresas, mas mantendo ainda nesta fase uma lógica de separação de grupos entre estas entidades que não permitia que os utilizadores acedessem aos perfis dos grupos a que não pertenciam (Boyd & Ellison, 2007, pp. 9-10).

Só em setembro de 2006 é que o Facebook se tornou completamente aberto ao público permitindo uma total partilha de informação entre utilizadores, e desde então tornou-se um dos sítios mais ativos de todos os existentes na Internet.

Para muitos, o Facebook tornou-se uma experiência pessoal diária, tão normal quanto comer ou dormir. Nesta rede de comunidades interligadas navegam diariamente pessoas de todas as idades – desde os adolescentes aos idosos – para partilharem os seus pensamentos, frustrações, conquistas e aventuras quer seja com palavras, com imagens ou até com vídeo. É onde eles vão para narrar os acontecimentos das suas vidas, muitas vezes, com uma aplicação móvel para partilhar no momento exato onde estão, com quem estão e o que estão a fazer, ou simplesmente para acompanhar outros cujo percurso de vida se cruza, ou cruzou no passado, com o seu.

Não deixa de ser admirável a forma como os utilizadores estão dispostos a partilhar toda esta informação sobre si mesmos, e principalmente como o fizeram sobretudo nos primeiros tempos em que o Facebook se debateu com algumas dificuldades no que concerne à privacidade das suas contas. Certo é que o Facebook revelou muita capacidade de adaptação e de inovação e, mesmo sendo hoje uma empresa gigante cotada em bolsa, continua a portar-se de um modo quase semelhante a uma *startup* que procura sempre a nova grande ideia. Esta ambição fez com que tenha conseguido sempre esticar os limites do que é possível fazer na Internet e fê-lo sempre convidando, e não forçando, os utilizadores a aderir a cada nova funcionalidade. Não será por isso de estranhar que este seja atualmente uma força motriz da economia mundial e se assuma como um líder das RS, que continua ainda a crescer.

Figura 5 – Perfil no Facebook de Mark Zuckerberg, seu fundador e CEO desde 2004
Fonte: https://www.facebook.com/zuck

Atualmente existem centenas de RS operacionais espalhadas pelo mundo mas, segundo o último estudo realizado pela eBizMBA[4] em 1 de março de 2015, o *Top* dos 15 sítios das RS mais populares do mundo (Figura 6):

-é liderado pelo Facebook que conta com novecentos milhões de visitantes únicos diários (VUD);

-tem na segunda posição o Twitter, com trezentos e dez milhões de VUD;

-tem na terceira posição o LinkedIn com duzentos e cinquenta e cinco milhões de VUD;

-tem ainda nas posições seguintes, e com mais de cem milhões de VUD, o Pinterest, o Google+ e o Instagram;

[4] O eBizMBA é um sítio especializado na informação para as empresas que têm negócios na Internet.

-não inclui o Youtube, porque este é classificado numa outra categoria, a dos sítios de vídeos, na qual é líder destacado com 1.000.000.000 de visitantes únicos mensais (eBizMBA The eBusiness Guide, 2015).

facebook	**1 | Facebook** 900.000.000 VUD http://www.facebook.com	flickr	**9 | Flickr** 65.000.000 VUD http://www.flickr.com/
	2 | Twitter 310.000.000 VUD http://www.twitter.com/	Vine	**10 | Vine** 42.000.000 VUD http://www.vine.co/
LinkedIn	**3 | LinkedIn** 255.000.000 VUD http://www.linkedin.com/	Meetup	**11 | Meetup** 40.000.000 VUD http://www.meetup.com/
Pinterest	**4 | Pinterest** 250.000.000 VUD http://www.pinterest.com/	TAGGED	**12 | Tagged** 38.000.000 VUD http://www.tagged.com/
Google+	**5 | Google Plus+** 120.000.000 VUD http://plus.google.com/	ask.fm	**13 | Ask.fm** 37.000.000 VUD http://www.ask.fm/
tumblr.	**6 | Tumblr** 110.000.000 VUD http://www.tumblr.com/	meetme	**14 | MeetMe** 15.500.000 VUD http://www.meetme.com/
Instagram	**7 | Instagram** 100.000.000 VUD http://www.instagram.com	classmates	**15 | ClassMates** 15.000.000 VUD http://www.classmates.com/
	8 | VK 80.000.000 VUD http://www.vk.com/	Nota: **VUD** – Visitantes Únicos Diários	

Figura 6 - Top 15 dos sítios mais populares de redes sociais em março de 2015
Fonte: eBizMBA Rank - março 2015

b. A esfera de presença: individual ou organizacional

Na sua génese as RS foram criadas a pensar numa utilização individual tanto mais que, quando os utilizadores aderem a uma RS é-lhes solicitado que preencham alguns formulários compostos por perguntas relacionadas com o seu nome, a sua idade, a sua localização, os seus interesses ou até perguntas abertas que permitem apresentar-se de um modo mais personalizado. O seu perfil é então construído com estas respostas e adicionalmente, na maioria das RS é-lhes ainda solicitada a submissão de fotos de perfil no intuito de o tornar mais humano e ainda de conteúdos multimédia no intuito de lhe conferir um aspeto visual mais apelativo (Boyd & Ellison, 2007, p. 3).

Numa fase posterior, é-lhes solicitado que tentem identificar outros utilizadores, já existentes no sistema, com quem têm uma relação. O rótulo para esses relacionamentos difere mas os termos mais populares incluem "Amigos" ou "Contatos", e estes exigem normalmente uma confirmação bidirecional para o estabelecimento dessa relação, ou amizade. No entanto existem outros laços “apenas” unidirecionais os quais são por vezes rotulados como "Fãs" ou "Seguidores", apesar de alguns sítios também os designarem “Amigos” o que poderá conflituar de forma enganadora com o conceito anterior (Boyd, 2006).

Enquanto as funcionalidades e características tecnológicas das muitas RS existentes pouco diferem, as culturas subjacentes a elas são muito diversificadas e resultam de múltiplas combinações de interesses comuns que podem ser por exemplo políticos, profissionais, lúdicos, afetivos, entre outros. Outro aspeto diz respeito à homogeneidade da audiência sendo que, se em alguns casos não existe noutros é perfeitamente possível identificar traços comuns nos seus utilizadores sejam estes a sua linguagem ou os seus ideários baseados na raça, sexo, religião ou nacionalismo (Boyd & Ellison, 2007, p. 1).

A exibição das conexões dos utilizadores é a componente mais importante de qualquer RS. A lista de “Amigos” exibe hiperligações selecionáveis que nos encaminham para os perfis de cada um destes, permitindo ir desenhando o grafo da rede[5] à medida que os vamos visitando. Tal importância constitui a razão pela qual esta lista de “Amigos” está sempre visível na maioria das RS para todos quantos tenham permissão para visualizar o perfil do utilizador, e tal só poderá ser alterado caso o utilizador seja mais capacitado informaticamente e consiga alterar programaticamente o seu perfil para a ocultar. A RS LinkedIn constitui um caso raro oferecendo aos seus utilizadores uma funcionalidade que lhes permite optar por exibir ou não exibir a sua rede de amizades.

Depois, para além da partilha da informação que está disponibilizada em cada perfil com todos quantos vão recebendo permissões para o visitar, existe ainda uma segunda componente importante para o sucesso das RS e que tem que ver com as funcionalidades para, durante estas visitas, os utilizadores poderem interagir mutuamente. Neste particular a maioria das RS oferece duas funcionalidades: a primeira permite aos utilizadores deixarem mensagens nos perfis dos seus “Amigos”, a qual tipicamente é materializada pela introdução de “comentários” (ainda que esta designação possa variar nos diferentes sítios),

[5] Um grafo é uma representação visual de um determinado conjunto de dados e da ligação existente entre alguns dos elementos desse conjunto (Ahuja, et al., 1993).

e a segunda permite aos utilizadores enviar mensagens para outros utilizadores de forma semelhante à do correio eletrónico (Boyd & Ellison, 2007, p. 3).

Mas o sucesso dos *media* sociais levou-os a oferecer também às empresas uma forma fácil destas interagirem não só com os seus acionistas, mas também com potenciais investidores, analistas e demais partes interessadas. As capacidades de interação multilateral do Twitter, do Facebook ou do Youtube permitem-lhes ainda recolher informações sobre as partes interessadas e responder a estas em tempo real. Uma vez descobertas estas potencialidades as empresas passaram a usar os *media* sociais de cinco maneiras principais: para criar reconhecimento à sua marca, como uma ferramenta de gestão da reputação *online*, como ferramenta de recrutamento, como escola de novas tecnologias e como uma ferramenta de última geração para identificar oportunidades prospetivas.

c. Os riscos da utilização das redes sociais

Mas nem tudo o que resulta do inter-relacionamento de indivíduos e de empresas nas RS são vantagens. Segundo o Federal Bureau of Investigation (FBI) existem duas táticas diferentes para explorar as vulnerabilidades associadas às RS, e estas na prática podem até ser combinadas. A primeira, consiste na execução de ataques informáticos físicos levados a cabo por *hackers*, que desenvolvem código ou *software* malicioso que uma vez executado ou instalado, lhes permite ter acesso ou controlar um computador ou telefone. A segunda, consiste numa exploração das ligações pessoais existentes nas RS, levadas a cabo por *hackers* do domínio social ou humano, que se especializam na manipulação das pessoas através de interações sociais que parecem inofensivas e legítimas, seja pessoalmente, ou seja à distância. E fazem-no porque sabem que os seres humanos são o elo mais fraco na segurança cibernética, e tentam enganar as pessoas para obter um meio de passar através dos mecanismos de segurança informáticos (FBI, s.d.).

Alguns dos riscos associados a estes esquemas ou violações de segurança informática são a disseminação de vírus ou *malware*, a alteração de conteúdos em sítios da Internet, o assédio, o roubo de identidade, o roubo de bens, o roubo de propriedade intelectual, o roubo de informação confidencial, entre outros, e estes podem resultar para os indivíduos na degradação da sua reputação pessoal ou profissional, e até na perda do seu emprego, e podem resultar para as empresas em roubo da imagem corporativa, degradação da reputação empresarial, danos em redes de dados ou em informação, atrasos ou interrupção da produção ou perda de receitas ou lucros (FBI, s.d.).

Analisar sinteticamente uma experiência conduzida nos EUA em dezembro de 2009, por uma empresa de cibersegurança chamada *Provide Security*, permite identificar claramente estas vulnerabilidades. Essa experiência, que ficou conhecida como "A experiência Robin Sage", veio demonstrar inequivocamente que nas RS existe um perigo real de fuga de informação, alimentado pela confiança que tendemos a depositar em alguém que outros com quem temos uma relação conhecem. Thomas Ryan foi quem liderou esta experiência e durante vinte e oito dias criou vários perfis, no Facebook, no Twitter e no LinkedIn, para uma pessoa que simplesmente não existia, usando para o efeito um conjunto de fotografias de uma mulher jovem e atraente que assumia ser uma especialista em cibersegurança e se chamava Robin Sage. Assumindo o controlo destes perfis e sendo ele próprio conhecedor profundo destes assuntos, iniciou um processo de contatos e estabelecimento de "amizades" com outros especialistas de cibersegurança, os quais, pela sua formação ou experiência teoricamente deveriam estar protegidos contra uma ameaça deste tipo. Aderindo às RS, registando-se em listas de correio eletrónico e enunciando credenciais falsas, conseguiu então criar as condições para investigar como é que estas pessoas tomavam decisões no sentido de confiar e partilhar informações com a identidade falsa (Ryan, 2010, p. 2).

O principal fator observado foi a possibilidade real existente de explorar o nível de confiança de outros indivíduos com base no género, ocupação, habilitações literárias, graus académicos e amigos. No final da experiência a falsa Robin Sage tinha estabelecido centenas de conexões nas várias RS e estas incluíam executivos em entidades governamentais ligadas à defesa, na *National Security Agency* (NSA), no *Department of Defense* (DoD) ou em grupos relacionados com as Informações Militares, e ainda outros amigos importantes que trabalhavam ou estavam ligados a empresas listadas na "Fortune Global 500"[6]. Como resultado destas ligações, foram-lhe oferecidos presentes, oferecidos empregos estatais ou particulares, e feitos convites para falar em variadas conferências de segurança. Ficou assim em primeiro lugar evidente pela relação resultados/duração da experiência que a propagação de uma identidade falsa através dos sítios das RS pode ser extremamente rápida. Em segundo lugar, que a escolha deliberada de uma mulher jovem e atraente parece ter exposto o papel que o sexo e a aparência têm na confiança e entusiasmo das pessoas para estabelecer uma conexão com alguém. Em conjunto com a sua imagem, as credenciais listadas no seu perfil resultaram numa perceção de credibilidade, explorando

[6] Ranking anual das quinhentas empresas internacionais consideradas as mais ricas e lucrativas.

também a tendência das pessoas para tirar conclusões precipitadas. Por fim, ao alcançar um grande número de conexões Robin Sage teve a capacidade de identificar os indivíduos que estavam mais bem posicionados para fornecer a maior quantidade de informações, tendo por base o seu envolvimento com várias agências governamentais. Grande parte da informação revelada à Robin violou procedimentos tanto da segurança das informações como das operações (Ryan, 2010, p. 2).

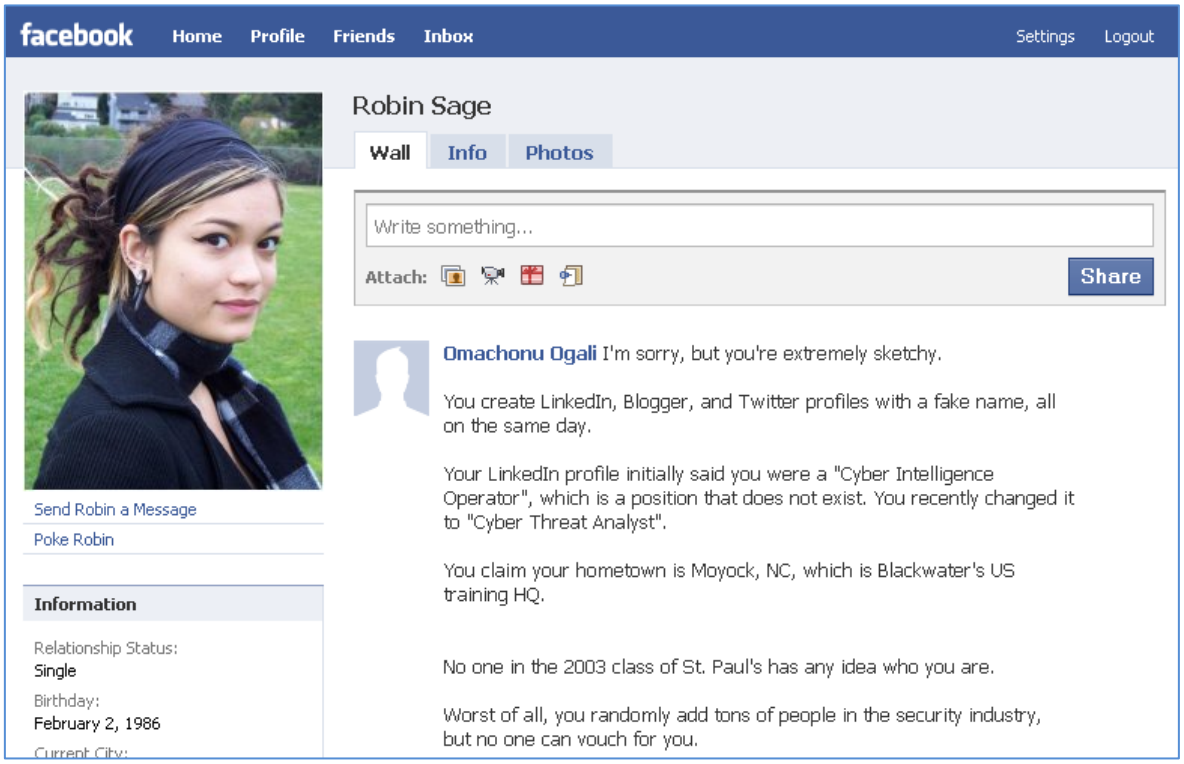

Figura 7 - Perfil no Facebook da Robin Sage, após ter sido desmascarado
Fonte: http://www.privacywonk.net/images/robinsage.png

Por alguma razão o nível de segurança que aplicamos às interações da nossa vida real decai quando estamos *online*. Na vida real, muito raramente falamos com estranhos acerca das nossas funções profissionais, especialmente se estas têm importância para a segurança nacional e estranhamente, talvez por se tratar do mundo *online*, parecia que ninguém se iria preocupar em submeter o perfil da Robin a uma investigação, simples de realizar, para testar se esta pessoa era de facto real ou até, se era um verdadeiro especialista. Durante toda a experiência apenas um indivíduo se propôs desmascarar a Robin (Figura 7), e segundo ele, foi a sua experiência profissional no campo da aquisição de informações que o levou a fazê-lo. Imediatamente pensou tratar-se de um nome falso quando recebeu o pedido de amizade no Facebook mas, isso por si só não o inquietou uma vez que é habitual algumas pessoas esconderem a sua verdadeira identidade por detrás de pseudónimos por

uma questão de proteção. Contudo, sabendo que os *hackers* também o fazem e por uma questão de precaução, decidiu questionar algumas pessoas conhecidas para saber se conheciam a Robin o que, descobriu contacto após contato, não acontecia. O passo seguinte foi procurar contatar outras pessoas no Facebook que tivessem frequentado os mesmos estabelecimentos de ensino que a Robin e que pudessem conhecê-la, mas esses contatos foram suficientes para perceber que esta simplesmente não existia (Lisko, 2010).

Normalmente as empresas ou organizações são os alvos mais apetecidos e são estas que sofrem os maiores prejuízos que resultam destes ataques pelo que são a parte mais interessada em compreender profundamente este fenómeno para, se poderem proteger. E para tal, primeiro terão obviamente que procurar conhecer os seus colaboradores, entender qual a utilização que fazem das RS e qual a sua consciencialização dos riscos que correm ao fazê-lo, quer para si, quer indiretamente para as suas empresas ou organizações. Posteriormente é necessário conceber um plano de segurança que reflita um conjunto de boas práticas e medidas protetivas para aplicar na sua atuação, garantindo a proteção da empresa mas sobretudo convencendo-os dos ganhos que eles próprios terão na sua segurança pessoal.

d. Os hábitos dos portugueses nas redes sociais

Segundo dados da estimativa de 1 de Julho de 2014 da Internet Live Stats[7] (Tabela 1), os portugueses ocupam a 53.ª posição no ranking mundial dos países com mais utilizadores da Internet. Tendo em conta que o total de utilizadores depende obviamente da população do país, esta variável não é a mais relevante para aferir o grau de envolvimento na Internet. Mas, considerando a taxa de penetração na população (Tabela 2), a qual mede o grau de adesão das pessoas à Internet de forma independente da população total do país, verificamos que Portugal desce ainda para uma pouco desejável 55.ª posição, muito atrás de outros países usados neste trabalho como referências, significando que temos ainda muito espaço para crescer e possivelmente com esse crescimento virá uma maior necessidade de criar regulamentação adicional.

A validade das conclusões tiradas por aqueles países e a aplicabilidade das medidas que estes criaram à realidade da defesa em Portugal, depende diretamente do grau de semelhança entre os hábitos dos utilizadores desses países e os dos portugueses, que a seguir se procura conhecer.

[7] Dados produzidos pelas *International Telecommunication Union* (ITU), *United Nations Population Division*, *Internet & Mobile Association of India* (IAMAI), e pelo *World Bank*, disponíveis em http://www.internetlivestats.com/internet-users-by-country/.

Tabela 1 - Ranking do número de utilizadores da Internet, por país, em 2014
Fonte: Internet Live Stats, Internet Users by Country, 2014

Rank	País	Nº Utilizadores	Δ anual (%)	População total	Δ anual (%)	Taxa penetração
1	China	641.601.070	4%	1,393,783,836	0,59%	46,03%
2	EUA	279.834.232	7%	322,583,006	0,79%	86,75%
3	India	243.198.922	14%	1,267,401,849	1,22%	19,19%
4	Japão	109.252.912	8%	126,999,808	-0,11%	86,03%
5	Brasil	107.822.831	7%	202,033,670	0,83%	53,37%
6	Rússia	84.437.793	10%	142,467,651	-0,26%	59,27%
7	Alemanha	71.727.551	2%	82,652,256	-0,09%	86,78%
8	Nigéria	67.101.452	16%	178,516,904	2,82%	37,59%
9	Reino Unido	57.075.826	3%	63,489,234	0,56%	89,90%
10	França	55.429.382	3%	64,641,279	0,54%	85,75%
---	---	---	---	---	---	---
53	Portugal	7.015.519	2%	10.610.304	0,02%	66,12%

Tabela 2 - Ranking da taxa de penetração da Internet, por país, em 2014
Fonte: Internet Live Stats, Internet Users by Country, 2014

Rank	País	Nº Utilizadores	Δ anual (%)	População total	Δ anual (%)	Taxa penetração
1	Bermudas	63.987	6%	65.461	0,18%	97,75%
2	Catar	2.191.866	13%	2.267.916	4,58%	96,65%
3	Barém	1.297.500	9%	1.344.111	0,90%	96,53%
---	---	---	---	---	---	---
15	Reino Unido	57.075.826	3%	63.489.234	0,56%	89,90%
---	---	---	---	---	---	---
18	Austrália	21.176.595	9%	23.630.169	1,23%	89,62%
---	---	---	---	---	---	---
25	EUA	279.834.232	7%	322.583.006	0,79%	86.75%
---	---	---	---	---	---	---
55	Portugal	7.015.519	2%	10.610.304	0,02%	66,12%

Segundo os dados apresentados na Figura 8, os quais fora extraídos do estudo da Marktest “Os portugueses e as Redes Sociais 2014” (Anexo A):

-o Facebook é onde 95,9% dos portugueses inquiridos estão presentes, ocupando a primeira posição deste ranking nacional de preferências (como se viu atrás também ocupava a primeira posição do Top 15 mundial);

-o Google+ é onde 41,1% dos portugueses estão presentes, ocupando a segunda posição (ocupava a quinta posição a nível mundial);

-o Youtube é onde 38,4% dos portugueses estão presentes, ocupando a terceira posição (não constava no Top 15 mundial);

-o LinkedIn é onde 31,4% dos portugueses estão presentes, ocupando a quarta posição (ocupava a terceira posição a nível mundial);

-o Twitter é onde 22,2% dos portugueses estão presentes, ocupando a 5ª posição (ocupava a segunda posição a nível mundial).

Pode concluir-se que em termos geográficos existem diferenças claras no grau de sucesso de cada uma das RS, pelo que, cada organização deverá considerar sempre um estudo adaptado à realidade nacional do seu país para adequar a sua política relativa às RS.

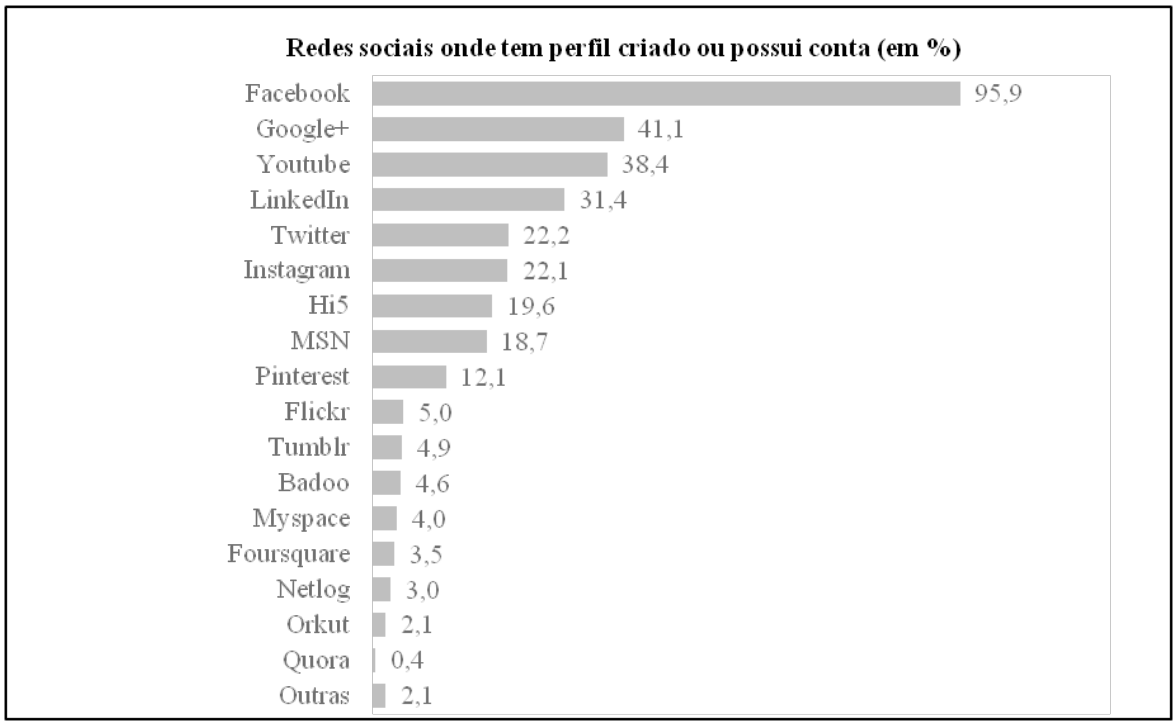

Figura 8 - Redes sociais onde os portugueses estavam presentes em 2014
Fonte: Marktest Consulting, Os Portugueses e as Redes Sociais 2014

Relativamente às funcionalidades que são utilizadas pelos portugueses durante a sua utilização das RS percebe-se pelos dados do mesmo estudo (Figura 9), que poucos são os que as utilizam apenas para difundir informação de sentido único, estando as três funcionalidades mais utilizadas diretamente ligadas à interação de grupo.

O âmbito dessa interação envolve sobretudo pensamentos, acontecimentos ou gostos pessoais enquadráveis no uso privado das RS, mas poderá envolver questões profissionais caso se trate de uma "Amizade" estabelecida entre colegas de trabalho. Nesses casos, muitas vezes as fronteiras profissionais podem ser distorcidas e podem por exemplo deixar as pessoas conhecer detalhes mais íntimos das suas vidas pessoais do que aqueles que seriam partilhados durante o horário de trabalho. Ou por exemplo, no caso das FFAA, tratando-se de uma instituição completamente hierarquizada o estabelecimento de "Amizades" no círculo social pode comprometer a capacidade efetiva de exercer o comando no ambiente "real" de trabalho.

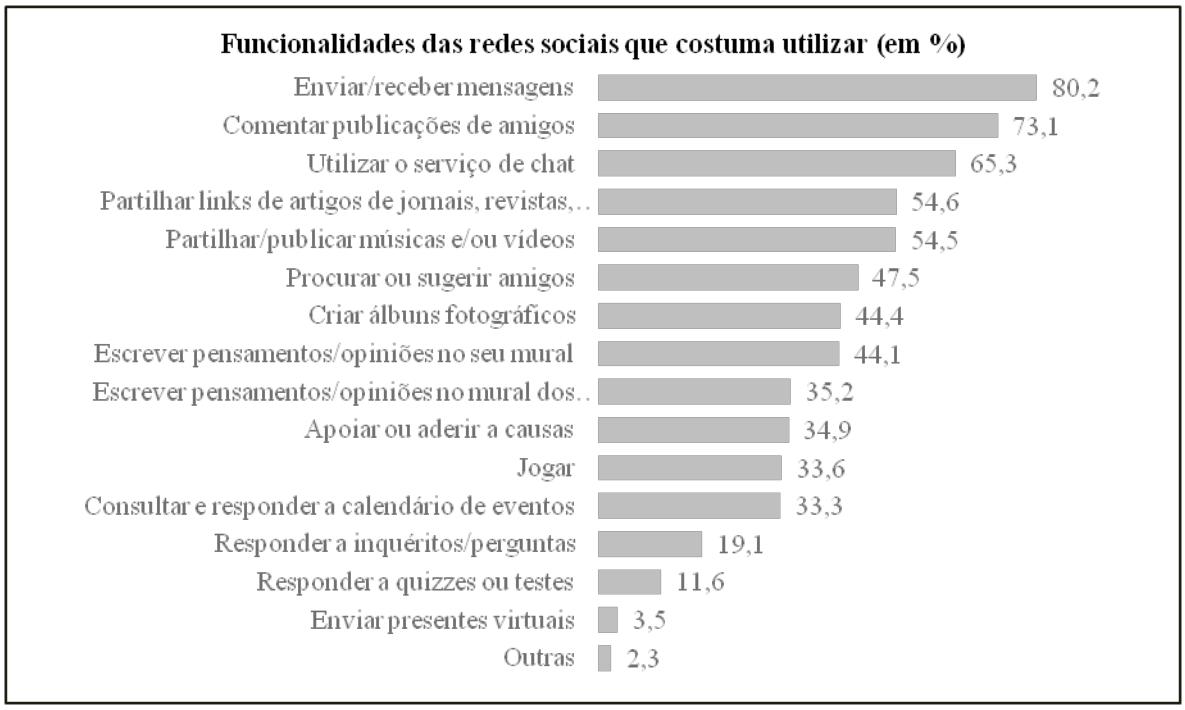

Figura 9 – Funcionalidades que os portugueses utilizavam nas redes sociais em 2014
Fonte: Marktest Consulting, Os Portugueses e as Redes Sociais 2014

Relativamente aos períodos de acesso às RS percebe-se (Figura 10), que cerca de metade as utiliza entre as nove e as 18 horas, naquele que pode se pode considerar o período laboral normal também para a defesa, mas que a grande maioria dos utilizadores é ao final do dia que aumenta a sua presença quando regressa a casa e ocupa o seu serão.

Excluindo situações de não atividade, associada a estudantes ou desempregados, estes dados pressupõe que muitas organizações e empresas permitem o seu uso no local de trabalho ou que a posse de equipamentos pessoais com ligação à Internet permite que estas ligações se façam de um modo permanente ao longo de todo dia. Outro facto surpreendente é existir um número muito substancial de utilizadores ligado durante a madrugada.

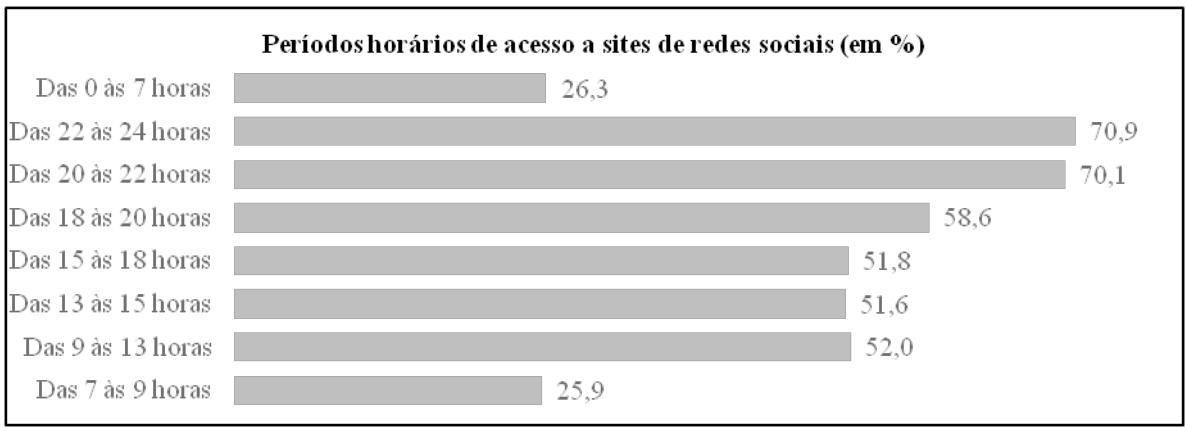

Figura 10 – Períodos horários em que os portugueses acediam às redes sociais em 2014
Fonte: Marktest Consulting, Os Portugueses e as Redes Sociais 2014

Relativamente ao tempo que é gasto nas RS diariamente (Figura 11) percebe-se que apenas 37,4% dos utilizadores não gasta mais do que 30 minutos por dia, que 50,1% dos utilizadores gasta entre meia hora e duas horas e que existem 12,5% dos utilizadores que gastam mais de duas horas por dia, o que poderá indiciar nestes alguma dependência.

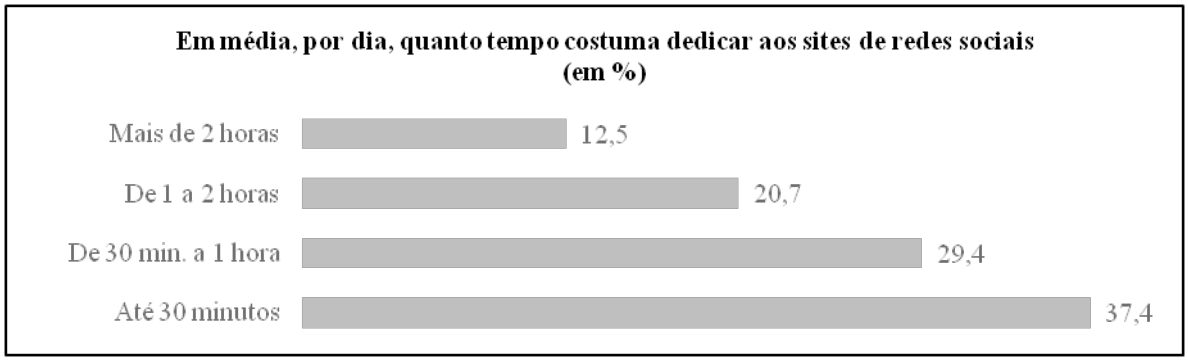

Figura 11 – Tempo de permanência dos portugueses nas redes sociais em 2014
Fonte: Marktest Consulting, Os Portugueses e as Redes Sociais 2014

Relativamente à frequência das visitas às RS (Figura 12) percebe-se que 84,3% dos utilizadores procura uma oportunidade para diariamente se ligar, e que 60,8% chegam inclusivamente a seguir as suas presenças várias vezes ao dia em períodos distintos, mantendo uma rotina de publicar ou obter informação quase em direto.

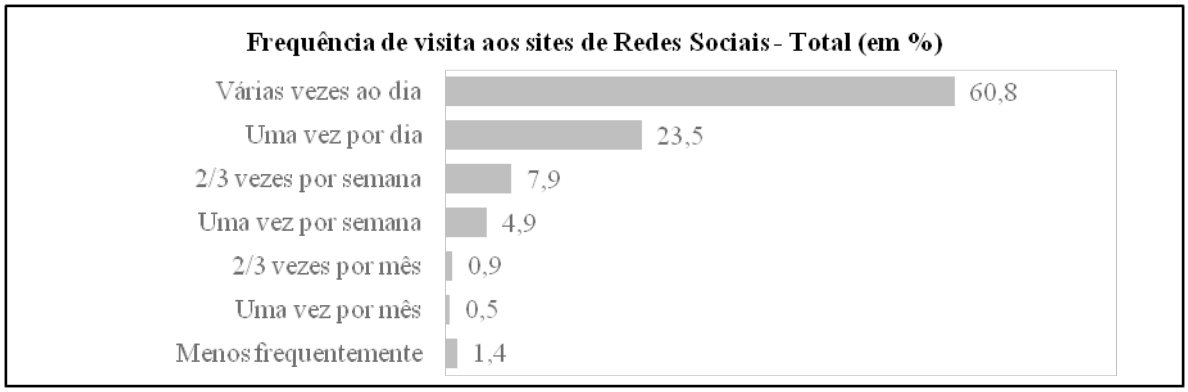

Figura 12 – Frequência de visita dos portugueses às redes sociais em 2014
Fonte: Marktest Consulting, Os Portugueses e as Redes Sociais 2014

e. Síntese conclusiva

Pelo que vimos atrás foi possível validar a H1. As RS são um fenómeno em contínuo crescimento, acompanhando o avanço tecnológico e explorando o desejo humano de se interrelacionar. Têm características distintas em termos geográficos e dinâmicas imprevisíveis sendo expectável que surjam novas plataformas ou que a importância das existentes possa vir a alterar-se, e envolvem completamente os portugueses que, estão quase todos presentes em pelo menos uma RS e fazem destas um uso quase diário, sendo algo que para muitos se tornou indispensável.

2. A utilização das redes sociais por elementos militares

a. A importância das Relações Públicas na defesa

Numa democracia é comum admitir-se que os cidadãos têm o direito de saber o que o Governo faz em seu nome e quais as razões que se encontram subjacentes. No que concerne à defesa em particular, é importante comunicar quais as atividades onde os seus recursos se encontram empenhados e que justificam o investimento do país para os manter, sobretudo num período em que se sente não existir uma ameaça real à segurança coletiva da nação.

Considerando ainda que nos últimos anos Portugal tem vivido uma grave crise económico-financeira, a gestão dos recursos das FFAA assumiu uma maior importância no plano de diminuição da despesa pública do Estado e colocou os esforços de ajustamento e reestruturação sob um maior escrutínio dos cidadãos e também dos *media*, os quais por vezes os exploram de forma incorreta, obrigando a defesa a tomar a iniciativa da comunicação e a saber lidar com estes efeitos.

Por outo lado, devido ao nosso modelo profissional das FFAA existe ainda uma necessidade contínua de assegurar a entrada de jovens nos quadros de pessoal, e o sucesso do processo de recrutamento destes jovens depende em grande medida da imagem que estes têm das suas FFAA.

É nestes campos que as RS se assumem como um canal privilegiado para as RP comunicarem eficazmente, fazendo-o hoje em dia através de campanhas de Marketing com a preocupação de melhorar o relacionamento com os cidadãos. Com o decurso do tempo, ocorreu uma importante transformação, deixando o Marketing de ter uma orientação exclusivamente virada para a produção ou para as vendas e passando a ter uma orientação focada nos desejos dos consumidores elegendo-os elemento chave da sua estratégia, e esta transformação alargou a aplicabilidade do Marketing para setores improváveis como o da defesa (Lahtinen & Isoviita 2001, 13).

Tendo em conta que os jovens de hoje podem ainda ser considerados nativos digitais, não é de estranhar que a defesa dos EUA tenha atribuído mesmo a alguns militares a missão de se tornarem *marketers* incentivando-os a envolverem-se nas RS. É esperado que nelas deixem uma mensagem positiva relativa às suas organizações e relativa à própria carreira militar, sempre com o foco no patriotismo como elo de ligação à restante comunidade. No entanto, é possível que tal atribuição cause alguns problemas do ponto de vista das RP, bastando para tal que alguns destes indivíduos não comuniquem de uma

forma ajustada às características especificas dos canais utilizados pelas RS, não estejam bem informados relativamente aos assuntos que tratam ou adotem opiniões ou visões distintas das oficialmente estabelecidas pelas chefias das suas organizações ou pela direção superior da defesa.

Dado que a cultura militar é conservadora, procura controlar cada detalhe que é divulgado sobre a organização. Os *media* sociais quebram o paradigma do controlo total da mensagem que é transmitida e talvez por isso algumas instituições da defesa não lidem bem com esse facto. O acesso a estes oferece a todos na organização, desde os generais aos soldados, a possibilidade de comunicarem para o mundo o que quer que lhes vá na alma, por vezes com benefícios mas noutras criando situações indesejáveis (Moe, 2011, p. 5).

b. A importância da Segurança da Informação na defesa

Para compreender o problema que a utilização das RS pode trazer à defesa será importante começar por analisar o conceito de segurança militar, e para tal, pode considerar-se a Publicação Doutrinária do Exército (PDE) 2-00 que define a Segurança como "A condição obtida quando a informação, o material, o pessoal, as atividades e as instalações estão protegidos contra a espionagem, a sabotagem, a subversão e o terrorismo, assim como contra perdas ou divulgações não autorizadas. A Segurança garante ao comandante, liberdade para planear e conduzir operações, reduzindo as vulnerabilidades às ameaças e atividades hostis. De igual modo, garantindo a segurança, o comandante ficará em melhores condições de conduzir as operações usando a surpresa. A Segurança contribui, de uma forma geral, para a FP[8], garantindo a manutenção do seu potencial de combate." (2009, pp. 2ª PARTE 1-2).

Da mesma publicação pode extrair-se que do conjunto de ameaças à segurança, existem as que são diretas, e que têm a ver com as levadas a cabo por um inimigo durante um conflito declarado, e as que são indiretas, e que têm a ver com as ações levadas a cabo por potenciais inimigos, em todo o espectro do conflito.

Isto é, no caso de existir um conflito as RS poderão mais facilmente ser consideradas uma ameaça e muito provavelmente os comandantes terão a necessidade de banir o seu uso, senão totalmente, pelo menos em momentos críticos das operações. No entanto, mesmo quando não existe um conflito latente, as ameaças de serviços de informações hostis, de organizações, grupos ou indivíduos subversivos ou terroristas, ou de organizações e grupos criminosos, mantêm-se.

[8] Proteção da Força, em inglês, *Force Protection.*

Excluindo-se a possibilidade de ocorrência da divulgação intencional de informação pelo próprio pessoal militar, da qual a defesa se protege verificando a lealdade do pessoal, e pondo em execução os procedimentos para a concessão de habilitações de segurança (credenciação) dos mesmos, existe a necessidade de identificar claramente qual a informação que tem de ser protegida e de educar os militares para não a divulgarem de forma não intencional na utilização da RS.

Todo este processo já faz parte do estabelecido doutrinariamente para a Segurança das Operações (OPSEC) que a publicação AJP 3-10 define como sendo "O processo que dá uma operação militar a segurança apropriada, utilizando meios passivos ou ativos, para negar o conhecimento ao adversário das disposições, capacidades e intenções de forças amigas. Em particular, a Seguranças das Operações é utilizada para identificar e proteger a informação que é fundamental para o sucesso de uma campanha, descrito como elementos essenciais de informação amiga (EEFI). Procura negar os EEFI ao decisor adversário, afetando assim a compreensão. Os EEFI vão precisar de ser protegidos durante todo o seu ciclo de vida e em toda a gama de operações militares. A vontade, compreensão e capacidade adversárias serão atingidas para manter a segurança dos EEFI, usando uma combinação de técnicas passivas e ativas." (OTAN, 2009, pp. 1-9).

A mesma publicação define ainda a Segurança da Informação (INFOSEC) "Sendo parte das OPSEC tem como objetivo proteger a informação (armazenada, processada ou transmitida), bem como os sistemas anfitriões, contra a perda de confidencialidade, integridade e disponibilidade através de uma série de controlos procedimentais, técnicos e administrativos. As INFOSEC incluem um conjunto de medidas que são aplicadas rotineiramente ao abrigo das políticas de segurança para proteger a informação." (OTAN, 2009, pp. 1-9).

São os regulamentos relacionados com a OPSEC e com a INFOSEC que protegem a defesa atualmente dos perigos relacionados com as RS, mas o carácter de informalidade destas atua como uma ameaça dissimulada que impede os militares de as detetarem e aplicarem os seus ensinamentos. Por outro lado o avanço tecnológico conduziu ao aumento da ameaça, já que a informação que circula sendo quase toda digital é infinitamente maior em volume, dificultando as medidas de controlo previstas pelas INFOSEC.

Olhando para um exemplo prático, em janeiro de 2010 o Ministério da Defesa do Reino Unido divulgou num relatório seu tornado público, que identificara nos 18 meses anteriores 16 ocasiões distintas em que ocorreram fugas de informação classificada não

intencional através de sítios das RS. Era então apontada como a principal causa para essas fugas de informação, a possibilidade de utilização livre das RS que os militares colocados no estrangeiro tinham em pontos de acesso livre à Internet instalados em *cyber* cafés, já que internamente a maior parte das redes de computadores administradas por este ministério não o permitia, e se vivia uma época em que eram poucos os dispositivos móveis com acesso à Internet (Garside, et al., 2012).

c. A busca de um compromisso na utilização das redes sociais pelos militares

Uma vez que os militares têm acesso aos *media* sociais numa base regular, existe o risco contínuo da revelação de informação, seja esta classificada ou apenas sensível, podendo comprometer as operações da defesa. Os militares têm liberdade para publicar, por exemplo, no Twitter ou no Facebook algo que numa questão de segundos passa a ser do conhecimento público e que, não pôde ser censurado nem pode ser apagado a não ser pelo próprio.

O sentimento que os militares extraem desta utilização dos *media* sociais é um sentimento de proximidade das suas famílias e dos seus amigos, e no processo, encaram com naturalidade a partilha de toda as informações pessoais, e esforçam-se para manter este fluxo contínuo alimentando o interesse dos outros por si e legitimando a manutenção do seu interesse pelas atualizações dos outros. Assim partilham informações sobre as suas vidas, os seus amigos, as suas famílias e até dos seus colegas, e tudo pode ser partilhado, até a submissão de fotografias instantâneas revelando as suas atividades e localização.

Na entrevista ao Major Paulo Mineiro, foi mencionada a tese de mestrado do Aspirante Dorotea Mutela, apresentada muito recentemente na Academia da Força Aérea, por conter algo particularmente interessante: o inquérito realizado a militares da Força Aérea (FA), utilizadores das RS e que participaram em missões internacionais, do qual foi possível extrair conclusões importantes[9]. Com estes dados terão conseguido perceber que muitos dos militares portugueses que utilizaram nas missões as RS, não tinham total consciência do que estava envolvido nessa utilização. Um exemplo disso é o facto de alguns possuírem *iphones* e desconhecerem que, de origem é feito o *tagging* das fotos com as coordenadas geográficas fornecidas pelo GPS do equipamento. Quando lhes foi perguntado se tinham cuidados com a utilização das RS durante a missão todos responderam que sim, mas de seguida foi-lhes perguntado se tinham publicado fotografias

[9] Não foi possível a cedência destes dados porque a tese ainda não foi aprovada para publicação pela FA.

tiradas com os seus *smartphones* e estes responderam afirmativamente. Porém, quando lhes foi perguntado se sabiam o que era o *geotagging* eles responderam que não.

O verdadeiro valor desta e de outras conclusões semelhantes é constituírem uma informação que, muito provavelmente, nem as FFAA nem a defesa tinham obtido até esta data de forma sustentada e utilizável para influenciar o processo de tomada de decisão no respeitante à interação com as RS. Se este tipo de investigação for alargado a mais militares certamente irá revelar falhas nos hábitos e na consciência securitária, comprovando a necessidade de se regular a utilização das RS, mas sobretudo de determinar quem são estes utilizadores para os procurar educar através de materiais educativos específicos para este tipo de problema.

Ao procurarmos responder à questão "quem são os militares que utilizam as RS nos ambientes de trabalho da defesa?" estaremos a identificar a dimensão do universo que constitui o objeto de estudo deste trabalho de investigação, e que se definiu como sendo os militares das FFAA portuguesas que se encontram na efetividade de serviço e que são utilizadores das RS.

Segundo os dados apresentados na Figura 13, retirados do último Anuário Estatístico da Defesa Nacional publicado pelo Ministério da Defesa Nacional português (2012), eram 31.111 militares os que se encontravam no ativo em 31 de dezembro de 2012.

Situação	Ramo das FA	Marinha	Exército	Força Aérea	TOTAL
QPa	Quadro Permanente (Ativo)	7.065	5.833	3.849	16.747
RC	Regime de Contrato	1.571	10.184	2.609	14.364
RV	Regime de Voluntariado				
	SUBTOTAL	**8.636**	**16.017**	**6.458**	**31.111**
QPrs	Quadro Permanente (Reserva)	1.533	1.151	855	3.539
QPrf	Quadro Permanente (Reforma)	7.516	8.709	3.916	20.141
	SUBTOTAL	**9.049**	**9.860**	**4.771**	**23.680**
	TOTAL	**17.685**	**25.877**	**11229**	**54.791**

Figura 13 – Pessoal militar, segundo regime e situação, em 31 de dezembro de 2012
Fonte: (Ministério da Defesa Nacional, 2012, p. 198)

Mas segundo o Art.º 150.º do Estatuto dos Militares das Forças Armadas (EMFAR) consideram-se na efetividade de serviço os militares no ativo que se encontrem em comissão normal ou na inatividade temporária por acidente ou doença (Ministério da Defesa Nacional, 1999) pelo que, dos anteriores iremos excluir 53, uma vez que dez se encontravam em comissão especial e 43 se encontravam de licença sem vencimento, como se pode constatar na Figura 14.

Ramo das FA Situação	Marinha	Exército	Força Aérea	TOTAL
Comissão normal	6.952	5.805	3.839	**16.596**
Comissão especial	4	2	4	**10**
Inatividade temporária	96	2		**98**
Licença sem vencimento	13	24	6	**43**
TOTAL	**7.065**	**5.833**	**3.849**	**16.747**

Figura 14 - Militares do QP no ativo, quanto à efetividade de serviço
Fonte: (Ministério da Defesa Nacional, 2012, p. 200)

Ou seja, considera-se que eram então 31.058 militares se encontravam na efetividade de serviço em 31 de dezembro de 2012.

O passo seguinte seria identificar quantos destes militares eram utilizadores das RS em ambientes de trabalho da defesa mas, a condicionante de não se poder utilizar outros instrumentos de observação que não entrevistas ou questionários *online* para o fazer de forma direta, restringiria desde logo o universo da amostra apenas aos utilizadores das tecnologias da informação, acabando por considerar que todos os militares são utilizadores da Internet. Não sendo ideal, podemos efetuar uma boa estimativa considerando que o estudo levado a cabo pela Socialbakers[10] identificou em Portugal, em 2012 (coincidindo com a data do anuário), uma taxa de penetração do Facebook na população *online* de 83,4% (inboundware.com, 2012).

Assume-se então como razoável estimar para efeitos académicos um número de 26.000 militares que são o objeto de estudo deste trabalho e a quem se teriam de se aplicar medidas para materializar os compromissos desejáveis na utilização da RS pelos militares de forma a minimizar os potenciais efeitos nocivos na conduta das operações e no relacionamento da defesa com os cidadãos, através do seu impacto na reputação e na imagem da organização.

d. Caso de estudo: a política de utilização das redes sociais norte-americana

A defesa dos EUA, através da publicação do *Directive-Type Memorandum 09-026* pelo DoD, em fevereiro de 2010, anunciou que era permitido o uso das RS tanto para fins privados como oficiais, o que significava unificar as diferentes estratégias que até esse momento cada serviço das FFAA norte-americanas havia seguido nesta matéria. Em termos mais práticos, significava que cada militar estava agora oficialmente autorizado a ter uma presença nas RS (a sua página, o seu perfil, o seu canal, etc.) e estava também autorizado a utilizar os computadores da defesa para lhes aceder no seu ambiente de trabalho. Ficava no entanto salvaguardada a possibilidade dos comandantes interromperem

[10] Socialbakers é o sítio mais popular de fornecimento de ferramentas analíticas, estatísticas e métricas para os *media* sociais.

temporariamente o acesso à Internet para preservar a Segurança das Operações ou para lidarem com problemas de falta de largura de banda. Era também mantida a obrigação destes negarem o acesso a sítios de RS que envolvam atividades proibidas tais como pornografia, jogo ou atividades relacionadas com o crime (2010).

Para as organizações militares isso significava que caso desejassem, podiam criar ou manter agora oficialmente as suas formas de presença nas RS, mas mais importante os *media* sociais passaram a ser uma parte integrante das operações do DoD, obrigando à criação de toda uma doutrina enquadrante e uma infraestrutura de supervisão e controlo dos conteúdos tornados públicos, capaz de orientar os responsáveis pela publicação dos conteúdos oficiais, de preventivamente dissuadir comportamentos irresponsáveis dos utilizadores e simultaneamente capaz de em tempo útil detetar situações potencialmente perigosas.

A operacionalização de tal estrutura começou com a criação de registos consolidados de todas as presenças oficiais de entidades ou colaboradores da defesa em sítios públicos dos *media* sociais. Foi o caso do Exército dos EUA que criou o sítio "*The U.S. Army on Social Media*"[11] onde passaram a constar todos os sítios autorizados a existir oficialmente (Figura 15), tendo para isso sido revistos e aprovados pelo Gabinete do Chefe de Relações Públicas do Exército e ficado sujeitos a todas as suas políticas e diretrizes de segurança. Os requerentes das autorizações de presença continuaram a ser os responsáveis pela gestão dos conteúdos de cada sítio nos *media* sociais, mas era esperado agora destes o cumprimento das regras estabelecidas pela segurança das operações ou das normas de conduta aplicáveis. Adicionalmente estes sítios passaram a ser monitorizados para tornar possível a deteção de eventuais incumprimentos, permitindo àquela organização conseguir numa primeira fase, rapidamente anular ou conter o problema e numa segunda fase, responsabilizar o causador do mesmo.

Como seria naturalmente desejável, o mecanismo de adesão a este diretório é muito simples e envolve apenas o preenchimento de um pequeno formulário *online* indicando as *links* dos sítios que procuram a autorização, um endereço de correio eletrónico e um contato telefónico da pessoa responsável por estes. No entanto é solicitada ainda a confirmação do conhecimento e concordância com o documento intitulado "*U.S. Army Social Media Registration Checklist*", designado no formulário como "*Submission*

[11] Disponível em http://www.army.mil/media/socialmedia/.

Guidelines", onde constam uma série de pré-requisitos necessários para a autorização (U.S.Army, s.d.).

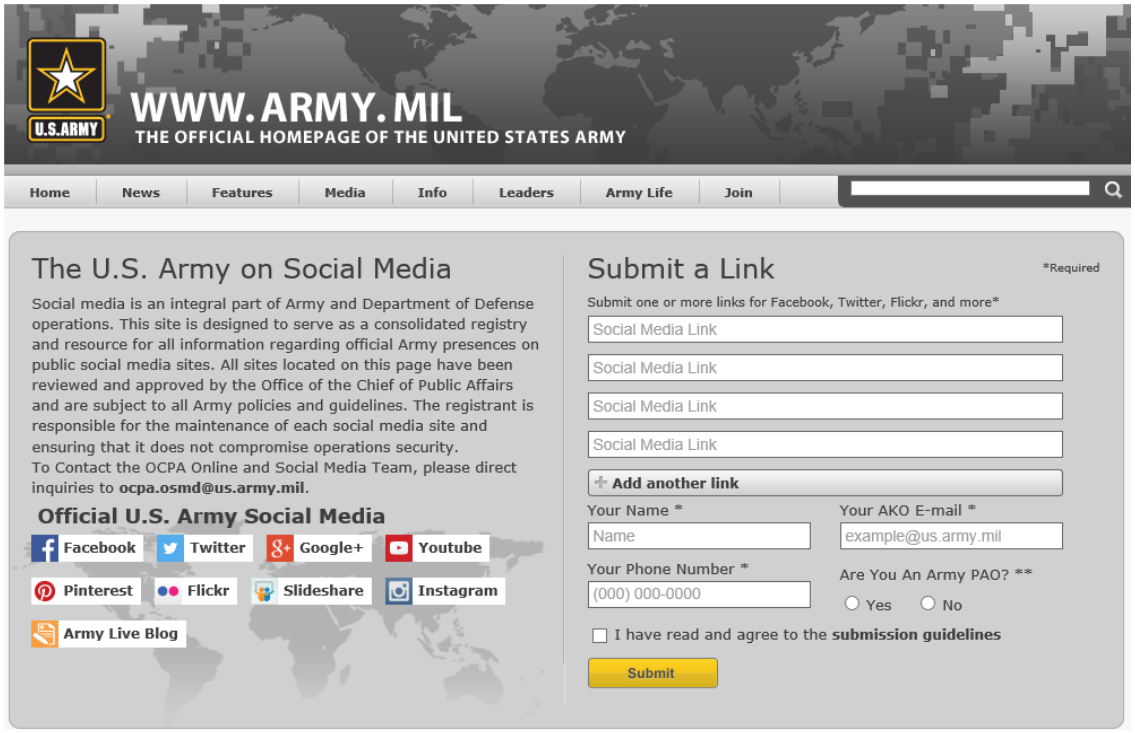

Figura 15 - Diretório das presenças oficiais do Exército dos EUA em sítios públicos dos *media* sociais
Fonte: http://www.army.mil/media/socialmedia/

Por outro lado, foi criada uma publicação de 52 páginas intitulada "*The United States Army Social Media Handbook*", cuja última versão é de março de 2014, e que constitui um completo manual educativo que prepara os militares para utilizarem as RS com consciência dos riscos que existem e de que só a sua conduta os pode eliminar, e que para além de si, quer a sua família quer os seus amigos podem substitui-lo como ameaça quando partilham nas RS informação sobre si (U.S. Army, 2014).

Nesta publicação todo o fenómeno das RS é explicado, o seu uso é incentivado, é dada ajuda para estabelecer novas presenças ou melhorar as existentes, é estabelecida uma separação entre o que são as presenças oficiais e as restantes (procurando esclarecer o papel de quem gere as primeiras e sobretudo mostrando o que não deve ser usado nas segundas), e são estabelecidas normas de conduta que devem ser seguidas para evitar situações indesejadas. Todo este material educativo é disponibilizado abertamente através da Internet e tem um formato apelativo e de fácil interpretação, para permitir a sua divulgação a todos os utilizadores independentemente do seu posto ou formação.

Mas será que todos estes esforços permitiram que os militares dos EUA pudessem utilizar as RS sem comprometer a sua segurança ou a das operações militares, ou causando

embaraços à defesa? Casos recentes, como o já referido dos militares da *Wisconsin National Guard*, demonstraram que na verdade não, e obrigaram o DoD a ter de efetuar uma reavaliação das metas e objetivos iniciais dessa autorização para determinar por que razão a defesa deve arriscar o uso das RS.

Esta reavaliação revelou duas razões primárias que justificam a necessidade de manter esta aposta: em primeiro lugar, a defesa precisa das RS para comunicar as suas atividades de informação e influência de forma mais eficaz, e em segundo lugar, as RS assumem-se como o principal meio através do qual os militares destacados mantêm contato com os seus amigos e familiares tornando-se um elemento vital para a manutenção do moral. Desta forma a própria instituição não tem outra alternativa senão esforçar-se mais para instruir os seus militares de forma a mitigar os riscos existentes (Moe, 2011, p. ii).

e. Síntese conclusiva

Do que anteriormente se expôs, conclui-se que a utilização segura das RS é uma utopia mas mesmo assim, cabe à defesa preparar-se para mitigar estes riscos e tal passará obrigatoriamente pela definição de uma política comum para a utilização das RS no geral, aplicável a todas as entidades ou organizações sob a sua tutela, e pelo estabelecimento de umas normas de conduta aplicáveis aos militares que utilizam as RS no seu ambiente de trabalho.

Foi também possível validar a H2, que estabelecia que “A tecnologia está cada vez mais presente nos ambientes de trabalho da defesa e o uso das RS em simultâneo nestes ambientes aumenta fortemente a ameaça à segurança da informação” já que a informação que circula nestes ambientes é cada vez mais digital e como tal fica mais vulnerável à sua divulgação através das RS.

3. A conceção de uma política comum de utilização das redes sociais

A expressão ganha pelas RS veio exigir que organizações se esforçassem para compreender o fenómeno e se adaptassem convenientemente. Dado existir todo um conjunto de novas ferramentas e plataformas emergentes, as melhores políticas para os *media* sociais são independentes destas, e estabelecem objetivos e métricas que suplantam qualquer RS em particular, já que a dinâmica que as caracteriza leva a que as que hoje existem e têm mais notoriedade, possam em pouco tempo deixar de ser relevantes ou simplesmente de existir.

Por outro lado, as organizações devem procurar suavizar tais políticas, transformando-as mais num conjunto de orientações, do que propriamente em regulamentos cujo desrespeito sujeita os seus colaboradores a sanções disciplinares punitivas. Em última análise, estas devem procurar educar os colaboradores ensinando-os a usar o bom senso enquanto utilizam os *media* sociais. Será ainda necessário estabelecer uma fronteira de separação entre a política de utilização que deverá ser aplicada ao pessoal que utiliza as RS no cumprimento das suas funções profissionais, e a que deverá ser aplicada a todo o pessoal quando faça uso das mesmas para fins privados.

a. A realidade da defesa em Portugal

A defesa em Portugal não definiu até ao momento um plano estratégico para os *media* sociais, o que deixa espaço para decisões autónomas dos diferentes decisores no estabelecimento de regras aplicáveis a esta matéria e, tal situação só pode resultar numa utilização perigosamente desregulada. As consequências desta desregulação serão naturalmente mais graves por se tratar de um setor muito particular, que impõe algumas limitações ao uso pleno das RS pelas características próprias de segurança que o tornam sensível a questões de perda de confidencialidade ou, pelas características de informalidade e profundo alcance das RS, que o tornam sensível ao desrespeito do decoro militar por via da adoção de condutas pessoais impróprias por parte dos militares.

Relativamente ao universo de organizações pertencentes à defesa, cada organização tem a sua própria estratégia e não existe cooperação entre elas a respeito quer de práticas comuns quer de troca de experiências baseada nas lições aprendidas individuais. Por outro lado, nem todas as organizações tomaram a decisão de estarem oficialmente presentes nas RS, o que se explica por estas constituírem canais alternativos aos sítios oficiais na Internet, que todos sem exceção possuem e utilizam amplamente para, manter o contato

com os cidadãos, manter o contato com o universo dos ex-militares ou ainda para servir de plataforma de recrutamento dos recursos humanos necessários para a sua operação.

As que estão presentes, e que são o próprio Ministério da Defesa Nacional, a Marinha e a Força Aérea optaram por estar em RS como o Facebook, o Youtube, o Twitter e o Flickr (Figuras 16, 17 e 18), baseando as suas decisões no grau de sucesso destas RS mas também em aspetos práticos de utilização, como acontece com o Twitter para ligação aos órgãos de comunicação social, já que estes privilegiam a rapidez de transmissão das notícias que este permite.

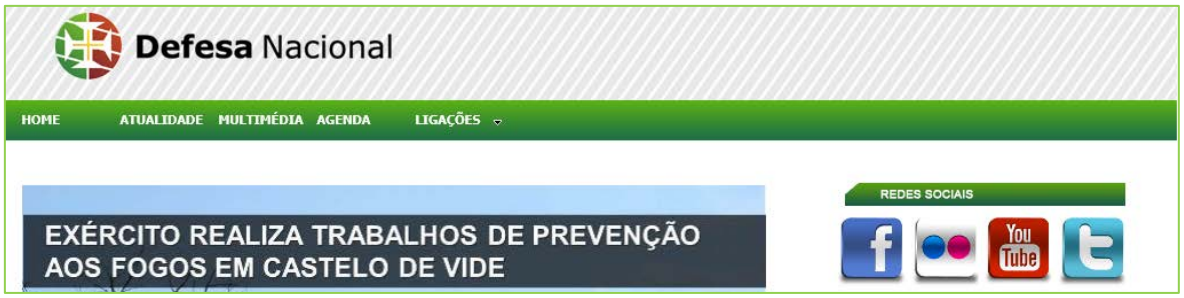

Figura 16 – Sítio da Defesa Nacional na Internet
Fonte: http://www.defesa.pt

Figura 17 – Sítio da Marinha portuguesa na Internet
Fonte: http://www.marinha.pt

Figura 18 - Sítio da Força Aérea portuguesa na Internet
Fonte: http://www.emfa.pt

Outra diferença significativa entre organizações reside nas diferentes políticas de acesso às RS nos computadores da defesa, as quais variam desde a total liberdade de utilização (que sendo particularmente importante nas missões no estrangeiro é comum, mas

que nos restantes ambientes de trabalho acaba por se tornar uma exceção), até à restrição total de acesso através da criação de filtros que impedem o acesso aos principais sítios das RS, ficando este reservado apenas para os militares que por inerência das suas funções utilizam as RS profissionalmente. Todavia, em quaisquer circunstâncias é salvaguardada a possibilidade dos comandantes bloquearem este acesso, sempre que entenderem existir essa necessidade.

O que todas têm em comum é o facto de não terem ainda desenvolvido normas de conduta, oficialmente aprovadas e distribuídas globalmente, nem terem desenvolvido um plano de formação para as aplicar. O que tem sido feito no sentido de educar os militares é realizar esporadicamente sessões de esclarecimento e sensibilização, destinadas a audiências selecionadas como o são os militares que se preparam para integrar forças nacionais destacadas.

Um fator positivo é que a experiência acumulada nas RS nos últimos anos tem ensinado àquelas organizações como devem atuar perante as singularidades da comunicação mais informal daqueles canais, como foi destacada a título de exemplo na FA, a importância de não eliminar comentários indesejados que tenham sido publicados por outros na sua página, nem de procurar responder-lhes em tom de defesa, já que a defesa mais favorável virá de forma natural das vozes da comunidade de utilizadores que, sentindo-se ligada à instituição por laços de afetividade, a irá defender.

b. A criação de uma *framework* para a política de utilização

(1) As regras militares subjacentes à criação de umas normas de conduta

O documento base que regula os comportamentos dos militares em qualquer circunstância da sua vida é o Regulamento de Disciplina Militar (RDM), e neste não existe lugar a qualquer separação entre as esferas da vida profissional e da vida pessoal do militar que se encontre na efetividade de serviço, já que o imperativo constante é o da condição militar ser indissociável da pessoa. Na sequência do "pacote legislativo" relativo à Defesa Nacional e às Forças Armadas que o atual governo se propôs rever, foi publicado em 22 de julho de 2009 o novo RDM, revogando o que estava em vigor desde 1977 (Decreto-Lei n.º 142/77 de 9 de Abril) e é nele que se devem procurar identificar quaisquer referências a limites de expressão ou a proibição de comportamentos ou atitudes que possam ser aplicáveis à utilização das RS.

Assim, começando pelo seu Capítulo I – Disposições gerais, encontramos as seguintes referências que podem ser relevantes nesta matéria:

-no art.º 2.º, Disciplina militar, ao "respeito dos princípios éticos da virtude e da honra inerentes à condição militar";

-no art.º 3.º, Sentido da disciplina militar, ao "estado de espírito coletivo assente no patriotismo, no civismo e na assunção das responsabilidades próprias da condição militar" que são a base da disciplina militar enquanto "elemento essencial do funcionamento regular das Forças Armadas";

-e no art.º 7.º, Infração disciplinar, a que "Constitui infração disciplinar o facto, comissivo ou omissivo, ainda que negligente, praticado em violação de qualquer dos deveres militares" (Assembleia da República, 2009, pp. 4667-8).

Já no seu Capítulo II – Deveres militares, serão particularmente importantes as seguintes referências:

-no art.º 11.º, Deveres gerais e especiais, a que "O militar deve, em todas as circunstâncias, pautar o seu procedimento pelos princípios da ética e da honra, (…) e pela obrigação de assegurar a dignidade e o prestígio das Forças Armadas" e que entre outros "São deveres especiais do militar" os deveres de zelo, de responsabilidade, de isenção política, de sigilo, de correção e o de aprumo;

-no art.º 17.º, Dever de zelo, a que "incumbe ao militar (…) Participar, sem delongas, à autoridade competente a existência de algum crime ou infração disciplinar que descubra ou de que tenha conhecimento";

-no art.º 19.º, Dever de responsabilidade, a que cabe ao militar "assumir uma conduta e uma postura éticas que respeitem integralmente o conteúdo dos deveres militares";

-no art.º 20.º, Dever de isenção política, a que cabe ao militar "um rigoroso apartidarismo, não podendo usar (…) o seu posto ou a sua função para qualquer intervenção política, partidária ou sindical;

-no art.º 21.º, Dever de sigilo, a que cabe ao militar "guardar segredo relativamente a factos e matérias de que o militar tenha ou tenha tido conhecimento, em virtude do exercício das suas funções, e que não devam ser revelados, nomeadamente os referentes ao dispositivo, à capacidade militar, ao equipamento e à atividade operacional das Forças Armadas, bem como, os elementos constantes de centros de dados e demais registos sobre o pessoal que não devam ser do conhecimento público";

-no art.º 23.º, Dever de correção, ao "tratamento respeitoso entre militares, bem como entre estes e as pessoas em geral" incumbindo ao militar "Não praticar, no serviço ou fora dele, ações contrárias à moral pública, ao brio, ao decoro militar e às práticas sociais; (…)

Ser moderado na linguagem, (…) não perturbar a ordem nem transgredir qualquer norma de direito em vigor no lugar em que se encontrar, não ofendendo os habitantes nem os seus legítimos direitos, crenças, costumes e interesses";

-no art.º 24.º, Dever de aprumo, a que cabe ao militar uma "correta apresentação pessoal, em serviço ou fora dele, nomeadamente quando se faça uso de uniforme" (Assembleia da República, 2009, pp. 4668-70).

Pelo que se conclui que, as situações relacionadas com o desrespeito pelo RDM e que podem sujeitar os militares a sanções disciplinares são genericamente: desrespeito pelos princípios da honra e da virtude, antipatriotismo, falta de civismo, atentado à dignidade e ao prestígio das FFAA, manifestação de opiniões políticas, quebra de respeito para com outros militares, revelação de provas (vídeos ou fotografias) de condutas ou ações contrárias à moral pública, ao brio ou ao decoro militar, ofensas através de linguagem imprópria ou de argumentos insultuosos dos direitos, crenças ou costumes da outras pessoas e por último a revelação de provas de uso incorreto de uniforme.

Para além destes, obviamente a quebra do segredo a que está obrigado aquando do manuseamento de informação relacionada com a defesa que seja classificada, ou que não o sendo, pela sua natureza possa ser sensível se chegar à posse de adversários ou inimigos.

(2) Princípios orientadores, normas de conduta e plano de formação

Segundo o estudo efetuado pela consultora George Patterson Y&R (2011) para a defesa australiana, para definir uma política para a utilização das RS pelos militares é necessário começar por definir os princípios orientadores da mesma, os quais devem ser separados em princípios aplicáveis aos militares que as utilizam para uso profissional e outros, aplicáveis aos que as utilizam para uso privado. Os princípios definidos naquele estudo resultaram da auscultação de uma equipa de aconselhadores legais, e podem perfeitamente ser tidos como ponto de partida para o caso português, cabendo a um futuro grupo de trabalho criado nesta área efetuar as eventuais adaptações necessárias. Estes princípios são remetidos para o Anexo B.

Depois de assimilados aqueles princípios, a *framework* para a implementação eficaz de uma política de utilização das RS na defesa é composta por um conjunto de regras de acesso, de normas de conduta e dum plano de formação, aplicáveis aos militares utilizadores das RS.

As regras de acesso devem ter um consideração a necessidade de salvaguardar o acesso às RS nos computadores da defesa para todos os militares que dele necessitem para

as suas funções, e para os restantes apenas o garantir fora do horário de serviço, minimizando assim riscos de segurança desnecessários e não interferindo em questões de produtividade. Deve ser garantida no entanto a autonomia aos diversos comandantes para restringir esse uso sempre que se justifique.

As normas de conduta devem incorporar num documento único:

-os condicionamentos que resultam do RDM;

-o processo interno de aprovação de informação para publicação nas RS (é apresentado como exemplo o do DoD dos EUA no Anexo C);

-as técnicas recomendadas para a construção de páginas no Facebook (são apresentadas no anexo D as existentes na publicação "*The United States Army Social Media Handbook*");

-as técnicas recomendadas para a utilização do Twitter (são apresentadas no Anexo E as existentes na publicação "*The United States Army Social Media Handbook*");

-uma lista de cuidados a ter com a seleção dos conteúdos, e neste particular as recomendações emanadas pelo Ministério da Defesa Britânico (2011) são extremamente sintéticas e objetivas, referindo que os utilizadores devem no geral evitar falhas na OPSEC provocadas pela publicação de fotos ou vídeos que revelem localizações, intenções operacionais ou capacidades e especificações de equipamentos militares; identificar-se a si ou a outros quando estão operações; imagens que possam denegrir a reputação da sua organização; posturas agressivas, abusivas ou inapropriadas estando fardados;

-e ainda umas regras de segurança que reforcem a consciencialização dos perigos existentes (o Facebook define uma lista no seu guia de segurança as "Melhores Dicas para se manter seguro no Facebook", e estas são incluídas como exemplo no Anexo F).

Uma vez criadas as normas de conduta devem ser produzidos materiais educativos de apoio à sua implementação, e deve ser iniciado um programa de formação tão abrangente quanto possível, que inclua prioritariamente os novos militares, ao entrarem na instituição. O formato digital deverá ser o privilegiado para a distribuição dos materiais educacionais, sobretudo por uma questão de custos, mas deverá ser equacionado o recurso ao formato impresso se este permitir reforçar o contato direto dos utilizadores com esta informação.

(3) O contributo individual na monitorização de comportamentos incorretos

Qualquer militar, uma vez consciente dos perigos existentes na utilização das RS e uma vez conhecedor das regras estabelecidas pela defesa para os mitigar, transforma-se a si próprio num valioso elemento na linha da frente da monitorização do que se passa nas RS e

fá-lo através do seguimento das suas conexões. Isto é, poderá caber-lhe um papel diferente daquele que se considerou até aqui e que retratava o militar como o potencial perpetrador, passando este agora a potencial delator da existência de conteúdos indesejados ou lesivos publicados por outros.

Através da sua ação poderá vir a contribuir de duas formas distintas para o bom uso das RS e da preservação do bom nome da sua organização, dependendo da exposição que tais conteúdos tenham sofrido.

O primeiro caso será aquele em que tais conteúdos já foram tornados públicos, e se trata apenas de ganhar tempo restando à organização tomar medidas de contenção do problema, as quais poderão vir a ter mais sucesso se tomadas mais perto dos acontecimentos. Nesse aspeto qualquer militar poderá ser o primeiro a dar o alerta, contatando para o efeito a sua organização.

O segundo caso será aquele em que tais conteúdos ainda não foram tornados públicos mas foram partilhados no seio de um grupo restrito a que o militar tem acesso. Considerando que as RS privilegiam as conexões mais próximas para efetuar a partilha de informações de uma forma mais reservada, particularmente quando se julga que o que se diz não deveria ser dito publicamente, cria-se um primeiro anel de contenção formado pelos “Amigos” que têm permissão para visualizar esses conteúdos. O cenário mais perigoso que se poderá colocar nesse ponto é o de alguém do grupo, autorizado a ver esse conteúdo, o replicar para terceiros tornando público esse conteúdo.

O dilema surge na ação que é possível o militar tomar quando se depara inicialmente com a situação, tendo de decidir se deve abordar diretamente o outro envolvido, procurando convencê-lo do erro que detetou e solicitando-lhe que retire respetivo conteúdo, ou se deverá contatar a sua organização para reportar o que foi detetado, confiando posteriormente nesta a avaliação da situação e a definição das ações a tomar.

Considerando o que diz o RDM no seu art.º 17.º do Capítulo II, não restam dúvidas que o militar deve “participar, sem delongas, à autoridade competente a existência de alguma infração disciplinar que descubra ou de que tenha conhecimento”, pelo que a sua decisão deverá depender da sua certeza relativamente a tratar-se ou não de uma infração disciplinar.

c. A definição de uma política de monitorização organizacional

A monotorização das RS por parte da defesa constitui um requisito indispensável para mitigar situações de risco, ao permitir de uma forma pró-ativa intervir e minimizar o tempo da exposição dos conteúdos indesejados ou lesivos.

Seria natural que, uma vez considerada pelas chefias a necessidade de monitorizar os perfis relacionados com a defesa, os amplos recursos existentes na defesa fossem direcionados para esta tarefa. No entanto, antes de o fazer é necessário procurar resposta a duas questões importantes: se é tecnicamente possível monitorizar um número na ordem das dezenas de milhares de presenças nas RS, sendo obviamente necessário definir "o que" procurar e quais as técnicas para o fazer; e, se é legal fazê-lo ou se pelo contrário as leis aplicáveis, nacionais ou internacionais, criariam a oportunidade para serem iniciados processos judiciais por parte daqueles que tinham sido observados.

Relativamente às técnicas utilizadas para efetuar a monotorização, estas vão desde a consulta manual às presenças nas RS reconhecidas como propriedade de militares, feita normalmente aleatoriamente e incidindo apenas na parte dos conteúdos tornados públicos, até à utilização de avançadas ferramentas informáticas denominadas *web crawlers*[12], que percorrem todo o universo de páginas dos perfis dos utilizadores das RS em busca de determinadas palavras-chave ou frases, que possam estar ligadas à organização e à sua atividade.

Um exemplo deste último tipo de abordagem é o utilizado pelo *Department of Homeland Security* dos EUA, que o utiliza para procurar "sinais de terroristas ou outras ameaças contra os EUA". Contudo, mesmo que para estes fins e na sequência de um processo judicial interposto pelo *Electronic Privacy Information Center*[13], foram obrigados a divulgar publicamente a lista das palavras-chave ou frases que utilizavam naquele processo. Essa lista veio revelar muito da forma como o governo "patrulha" a Internet, e mais concretamente as RS, à procura de eventuais ameaças domésticas ou externas, sem que no entanto, fosse também revelado de que forma é que este órgão conseguiu ter acesso aos vários motores de busca e RS, ou quais as tecnologias que utilizou para conseguir obter extrair a informação de tão grande volume de dados (Cohen, 2012).

[12] Um *web crawler*,, também conhecido por *robot* ou aranha, é um sistema para efetuar o *download* de páginas de Internet em massa, sendo utilizado principalmente pelos motores de busca (Olston & Najork, 2010).
[13] Todos os documentos deste processo disponíveis em http://epic.org/foia/epic-v-dhs-media-monitoring/.

Poder-se-á no entanto supor que tenha de existir um acordo especial com companhias norte-americanas como o Facebook ou o Twitter nas RS, porque de outra forma estas têm apertados mecanismos de controlo que lhes permitem identificar quaisquer tentativas de vigilância de contas ou perfis em massa, e normalmente os seus departamentos jurídicos atuam imediatamente quando tal é detetado.

Um exemplo disso é o caso retratado pelo próprio Pete Warden, que sendo um engenheiro de *software*, conta no seu *Blog* como foi processado pelo Facebook depois de ter desenvolvido um programa, e durante seis meses o ter utilizado para efetuar a recolha de nomes de pessoas e as suas localizações. Tal como Warden descobriu, na justiça tende a prevalecer a ideia de que "a única forma legal de aceder a um sítio web usando um *crawler* é obter previamente uma autorização por escrito", coisa que ele não havia feito. Ele apenas havia seguido "a regra" que tem prevalecido na Internet e que consiste em respeitar o ficheiro armazenado pelo proprietário na raiz do seu sítio na Internet, designado "robots.txt", onde este inclui as partes do seu sítio que autoriza que um *crawler* pesquise (Figura 19). Warden pensava que ao tê-lo respeitado estaria protegido. A única solução passou por chegar a um acordo que envolveu a destruição da totalidade de dados que tinham sido extraídos (Warden, 2010).

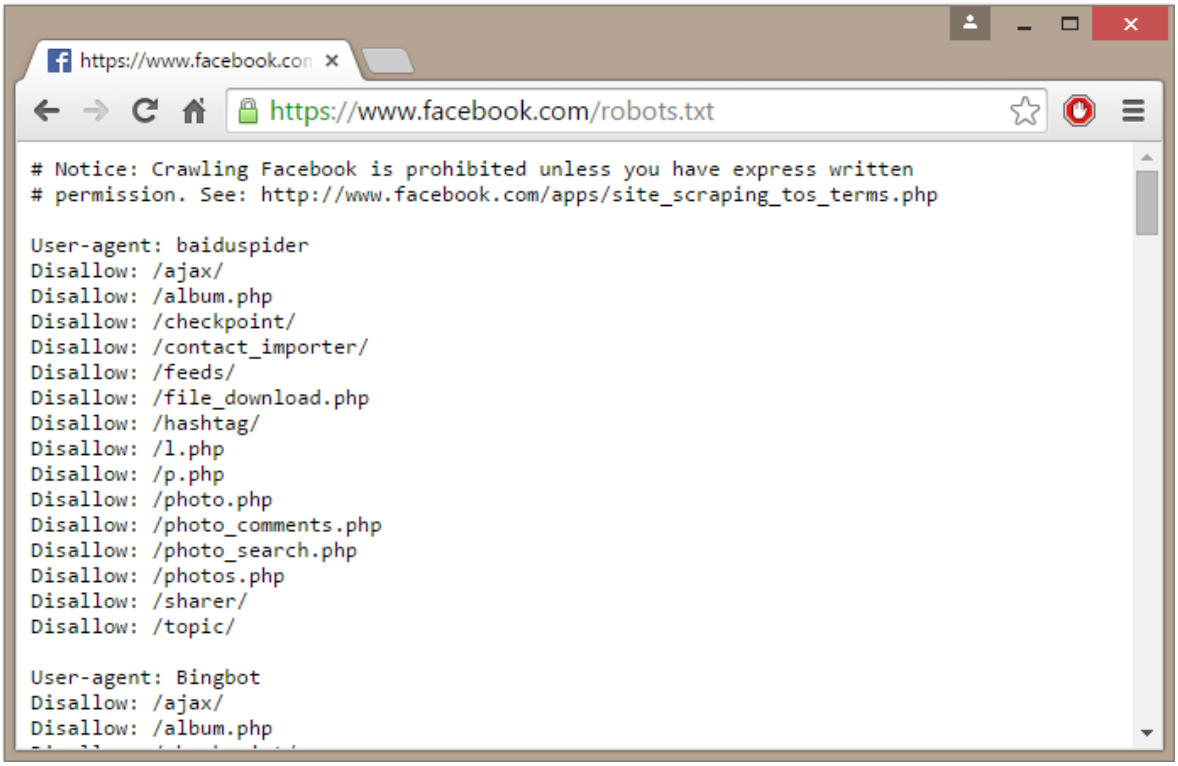

Figura 19 - Ficheiro que define as áreas do sítio do Facebook que podem ser acedidas por um *crawler*

Fonte: http://www.facebook.com/robots.txt

Esta questão de legalidade prende-se com a existência de direitos de proteção da informação dos utilizadores que obrigam à imposição de apertadas regras por parte das empresas proprietárias dos sítios das RS, como é o caso do Facebook, cuja base de dados dos seus utilizadores é o alvo mais apetecido da extração e interpretação de dados, muito valiosos para o marketing da generalidade das empresas.

Assim, para não correr riscos semelhantes a única solução para a defesa poder implementar uma politica de monotorização das RS é, tal como o Exército dos EUA fez, procurar a criação de um diretório dos sítios oficiais e incentivar os militares a aderirem a este, aceitando regras que na prática oferecem a cobertura para efetuar de forma legal uma monotorização daquelas presenças.

d. A utilidade da criação de uma rede social própria da defesa

A criação de uma RS própria da defesa apesar de não implicar grandes custos de instalação, traduzir-se-ia em mais um recurso para ser gerido pelos recursos humanos internos, normalmente escassos para estas áreas, e apenas permitiria deslocar uma pequena parte das interações que hoje são feitas por militares nas RS públicas para aquela plataforma, que sendo mais restrita se tornaria indiscutivelmente mais segura.

Mas, o propósito único da troca de informação entre os militares sobrepõe-se completamente às funcionalidades que já são hoje disponibilizadas nas *intranets* de cada organização, as quais possuindo capacidades colaborativas permitem facilmente criar espaços para partilha de conhecimento, facilitam o reconhecimento de especialistas existentes na organização, permitem criar fóruns de discussão, entre muitas outras.

Como tal, a vantagem que efetivamente possuem quando comparadas com as *intranets*, é que sendo sítios externos facilitam o contato com ex-militares, que de outra forma não lhes poderiam aceder. Mas por outro lado é possível visualizar duas desvantagens que afastariam muitos potenciais utilizadores:

-uma funcionalidade típica daquela rede seria a indicação de presença, que se traduz num indicador visual que mostra a presença de um elemento *online*, e que poderia basicamente transformar-se num sinalizador de presença do militar no seu posto de trabalho;

-na maioria dos sítios de RS, o registo é aberto a qualquer utilizador, e cada membro ao fazer o registo é colocado ao mesmo nível porque foram projetados para não terem hierarquia, pelo que a estrutura social da defesa, existente no mundo real que é totalmente hierarquizada, veria achatadas as suas ligações, podendo as interações acontecer

espontaneamente tanto no sentido horizontal da hierarquia quer no sentido vertical, e o valor das intervenções de cada um tenderia a ser exatamente igual contrariando o que normalmente se passaria no exterior.

Existe no entanto um caso de sucesso que é o da RS própria da defesa dos EUA, que se chama RallyPoint e foi fundada em 2012 por dois veteranos militares na Harvard Business School para ajudar a tornar a vida dos militares melhor e mais segura. Tendo contado com o apoio de dois dos últimos Chefes do Estado-Maior Conjunto das FFAA dos EUA, o RallyPoint conecta os seus membros e dá-lhes as melhores ferramentas para ter sucesso tanto no serviço militar, como também para encontrar oportunidades fora dele. Ali os militares podem construir a sua rede profissional tal como fariam noutra RS, mas vão conectar-se apenas com outros membros das FFAA e veteranos num ambiente seguro.

Devido à dimensão da estrutura de defesa norte-americana e à sua atividade intensa, que espalha os seus militares por todo o mundo, a utilidade desde tipo de plataforma pode justificar o investimento, mas em Portugal e na conjuntura atual dificilmente o justificaria.

e. Síntese conclusiva

Pelo que anteriormente se expôs foi possível validar a H3, que estabelecia que é necessário criar normas de conduta para os militares que utilizam as RS e que as semelhanças existentes nas diversas estruturas das FFAA aconselham à definição de uma política comum. Esta política deverá ser criada a partir de uma *framework* composta por um conjunto de regras de acesso, de normas de conduta e dum plano de formação, aplicáveis aos militares utilizadores das RS e ter em conta os condicionamentos impostos aos militares pelo RDM. A criação de uma RS própria da defesa não constitui um investimento atrativo uma vez que internamente será pouco convidativa e não substituirá as outras RS como se quereria para anular os riscos da sua utilização.

Conclusões e recomendações

a. Conclusões

O que se estudou permite responder claramente à QC do trabalho, que como se recorda é: "Em que medida as Forças Armadas devem permitir e regular o uso das RS em ambientes de trabalho no âmbito da defesa?". Uma vez conhecidos os perigos associados à permissão deste uso, os quais têm que ver com a possibilidade de num ambiente de trabalho onde toda a informação é cada vez mais digital se criarem pontos de fuga de informação que podem comprometer as atividades da defesa ou a segurança dos militares, conclui-se que o acesso livre às RS nos computadores da defesa, durante o horário normal de serviço, deve ser restringido apenas àqueles que delas façam uso profissional. Na esfera do uso privado, já existindo hoje tecnologias que permitem que os militares possam usá-las em qualquer momento nos seus próprios equipamentos, a defesa só deve restringir este uso em situações muito excecionais de carácter operacional (tendo como suporte o RDM) preocupando-se apenas em exercer todos os esforços para que os militares saibam utilizar estas redes de forma segura, e se possível até favorável para a imagem da instituição.

Não deixa de ser importante ressalvar que apesar da referência feita às políticas e às práticas regulatórias dos EUA nesta investigação, se deve ter a consciência que a realidade da defesa portuguesa obriga a olhar de modo diferente para a utilização das RS já que, a legislação dos EUA é um caso muito particular na salvaguarda de direitos e liberdades, e procura ser muito permissiva para ir sobretudo de encontro à liberdade de expressão.

Relativamente à regulamentação que é necessário criar, o estudo efetuado traz duas perceções importantes. A primeira, de que a importância que as RS assumem no contexto das relações entre pessoas, organizações é crescente e independente das tecnologias ou plataformas. A segunda, que a complexidade do estabelecimento de uma política eficaz de utilização das RS nos ambientes de trabalho da defesa, seja comum ou não, implicará grandes esforços sobretudo em recursos humanos, seja para monitorizar o que nelas se passa seja para implementar um plano de formação que envolva todos os militares. Neste particular, dada a característica idêntica dos desafios colocados às diferentes organizações da defesa admite-se que estes recursos humanos possam vir a ser partilhados.

Outro aspeto que ficou claro é que ao contrário de outras áreas de conhecimento, as preocupações a ter com a utilização das RS deverão ser comuns às diferentes organizações, variando apenas a mensagem institucional que cada uma quererá fazer chegar aos

cidadãos, fazendo crer que é viável e recomendável uma sinergia de esforços neste campo, para partilha de conhecimento e uniformização de procedimentos.

Tendo em conta o cenário atual, em que cada organização tem a sua própria estratégia e adota uma postura pouco colaborativa, poderá ser necessário que seja o próprio Ministério da Defesa a promover uma estratégia de cooperação entre as organizações de modo a convergir futuramente para uma solução, que permitisse por exemplo, olhar para a gestão das presenças nas RS como algo tão importante que, envolveria uma equipa combinada de elementos técnicos bem formados e a trabalhar nesta área em exclusividade, e a fazer um acompanhamento situacional vinte e quatro horas por dia, sete dias por semana, de tudo o que se passa nas RS e afeta a defesa.

Tal combinação de esforços está perfeitamente em linha com o que já foi defendido num nível superior para as diferentes nações. Num artigo da revista *NATO Review*, Tobias Franke[14] defendeu que o papel central que as RS têm atualmente nos países da União Europeia e da Organização do Tratado do Atlântico Norte (OTAN) justificariam "uma abordagem comum e uma estratégia partilhada entre as nações", capaz de "proteger os cidadãos das armadilhas da rede dos *media* sociais, e de, ao mesmo tempo, abraçar as oportunidades que representam para a expressão criativa". Para tal considerava que seria necessário empenharem-se numa nova linha de esforço, na qual as democracias Ocidentais se irão debater para mitigar os riscos que a utilização das RS representa para a segurança cibernética. Mas que para se ter sucesso era necessário que esta deixasse de descurar o papel dos *media* sociais, que até agora têm sido vistos como canais cibernéticos "suaves", ou seja de uma segunda linha de ameaças que não é considerada na definição de ameaça cibernética (Franke, 2011).

Ou seja, os mesmos argumentos utilizados para justificar a necessidade de unificar esforços e procedimentos ao nível da Defesa em Portugal, podem ser facilmente elevados ao nível da OTAN, já que os desafios que se impõem e os objetivos a alcançar são exatamente iguais. Acresce ainda que na conjuntura atual o papel que as RS têm desempenhado na proliferação da ameaça terrorista, traz um sentido completamente novo aos esforços que a defesa desenvolva futuramente para dominar uma área tão exigente e desafiante como se pensa ter ficado demonstrado, e que para o conseguir necessita de um investimento humano para reclamar um lugar mais forte neste domínio.

[14] Durante o mestrado em "*EU International Relations and Diplomacy Studies*" no *College of Europe*.

b. Recomendações

O Conceito Estratégico de Defesa Nacional, aprovado pela Resolução do Conselho de Ministros n.º 19/2013, estabelece que "o caráter predominantemente conjunto da atuação das Forças Armadas deve estender-se não só aos conceitos operacionais, à doutrina e aos procedimentos, mas também à cultura institucional e organizacional das Forças Armadas" o que "torna inadiável o aprofundamento da reforma das estruturas da defesa nacional e das Forças Armadas, através da maior integração de estruturas de comando e direção, de órgãos e serviços administrativos e logísticos" (Governo de Portugal, 2013).

Seguindo esta lógica, um esforço partilhado para desenvolver uma política comum de utilização das RS na Defesa, poderá criar uma base de uniformização muito útil para o caso de se vir a verificar a integração dos órgãos de Comunicações e Sistemas de Informação preconizada pela reforma estrutural, designada de "Defesa 2020"[15].

Do que se estudou recomenda-se que seja planeada uma campanha de informação com o objetivo de levar todo o pessoal ligado à defesa a registar as presenças nas RS que estejam a ser utilizadas com um carácter oficial, de modo a criar uma base de dados centralizada. Os administradores desses sítios ou páginas deverão registar também os seus dados para que seja possível acompanhar a atualização dos conteúdos aí publicados, mas sobretudo ajudar, em situações de impossibilidade ou incapacidade, a encontrar soluções para que estas presenças continuem a ser geridas e ativas.

Seguidamente deve ser iniciado um projeto com o objetivo especifico de criar umas normas de conduta comuns de utilização das RS pelos militares e todo um conjunto de material educacional necessário para os educar, levado a cabo por um grupo de trabalho conjunto, composto por elementos das diferentes organizações,

Uma vez criadas essas normas deve ser definida uma política de utilização das RS comum, já que se vê grande vantagem na uniformização, contribuindo esta para uma maior coesão através do sentimento de pertença a uma entidade comum que salvaguarda as especificidades de cada organização mas regula de forma igual aspetos comuns. Assim, em simultâneo com a distribuição das normas de conduta comuns e do material educacional seria implementada uma política de acesso às RS a horário, sendo-o permitido apenas fora do horário normal de serviço e durante o período do almoço, ficando garantida no entanto a autonomia aos diversos comandantes para restringir esse uso sempre que se justificasse.

[15] Resolução do Conselho de Ministros n.º 26/2013, que aprova as linhas de orientação para a reforma da defesa nacional e das Forças Armadas

Considerando que o número de utilizadores das RS na defesa foi estimado em cerca de 26.000 devemos considerar que a distribuição de material educacional no formato impresso só é exequível se tomar a forma de *flyer*, passando uma mensagem extremamente compacta, os quais não tendo de ser obrigatoriamente iguais para cada uma das organizações em termos de grafismo devem conter exatamente os mesmos elementos textuais. Estes deverão ser idealmente distribuídos numa ação coordenada no tempo em simultâneo em todas as organizações subordinadas à defesa, sendo-o preferencialmente nos locais de maior concentração de pessoas fora dos atos de serviço, o que poderá significar distribui-los por exemplo em bares ou messes existentes.

Complementarmente, o formato digital será utilizado para a distribuição dos restantes materiais educacionais, mais volumosos e pormenorizados, contendo as orientações aprovadas para todos os que sejam utilizadores das RS sendo aconselhável que, tal como acontece no caso americano (formato de apresentação na plataforma *Slideshare*) se utilizem os formatos mais interativos possível. A distribuição da informação considerada de uso interno deverá ser feita nos sítios da intranet e a considerada apropriada para ser tornada pública e por exemplo partilhada com as famílias, deverá ser feita na Internet.

Finalmente, uma vez atingidos os objetivos anteriores deverá ser implementada uma política de comunicação interna especificamente pensada para reforçar a boa imagem da organização junto dos próprios militares para que estes, na sua utilização das RS possam, agora de forma mais segura, continuar a atuar como verdadeiros embaixadores das suas organizações fazendo o eco das suas opiniões suplantar a mensagem menos original e sempre politicamente correta que caracteriza as RP.

Referências bibliográficas

Ahuja, R. K., Magnanti, T. L. & Orlin, J. B., 1993. *Network Flows: Theory, Algorithms, and Applications.* 1 ed. New Jersey: Prentice Hall.

Assembleia da República, 2009. *Lei Orgânica n.º 2/2009 de 22 de Julho.* Lisboa: Diário da República.

Boyd, D., 2006. *Friends, Friendsters, and MySpace Top 8: Writing community into being on social network sites. First Monday, 11.* [Em linha] Disponível em: http://www.firstmonday.org/issues/issue11_12/boyd/ [Consult. em 22 mar. 2015].

Boyd, D. & Ellison, N., 2007. Social network sites: Definition, history and scholarship. *Journal of Computer-Mediated Communication,* 13(1), pp. 210-230.

British Ministry of Defence, 2011. *Personal safety Em linha.* [Em linha] Disponível em: http://www.blogs.mod.uk/onlineecurity/index.html [Consult. em 24 mar. 2015].

Cohen, R., 2012. *Dept. of Homeland Security Forced to Release List of Keywords Used to Monitor Social Networking Sites.* [Em linha] Disponível em: http://www.forbes.com/sites/reuvencohen/2012/05/26/department-of-homeland-security-forced-to-release-list-of-keywords-used-to-monitor-social-networking-sites/ [Consult. em 31 mar. 2015].

Department of Defence, 2010. *Directive-Type Memorandum (DTM) 09-026 – Responsible and Effective Use of Internet-based Capabilities.* [Em linha] Disponível em: http://www.defense.gov/NEWS/DTM%2009-026.pdf [Consult. em 8 abr. 2015].

Department of Defence, 2012. *DoD Internet Services and Internet-Based Capabilities (DoDI 8550.01, September 11).* s.l.:U. S. Department of Defence.

Digital Trends Staff, 2014. *The history of social networking.* [Em linha] Disponível em: http://www.digitaltrends.com/features/the-history-of-social-networking/ [Consult. em 3 abr. 2015].

eBizMBA The eBusiness Guide, 2015. *The top world social networking sites.* [Em linha] Disponível em: http://www.ebizmba.com/articles/social-networking-websites [Consult. em 23 mar. 2015].

Exército Português, 2009. *PDE 2-00 Informações, Contra-informação e Segurança.* s.l.:Exército Português.

FBI, s.d. *Internet Social Networking Risks.* [Em linha] Disponível em: http://www.fbi.gov/about-us/investigate/counterintelligence/internet-social-networking-risks-1 [Consult. em 6 abr. 2015].

Franke, T., 2011. *NATO REVIEW magazine: Social media: the frontline of cyberdefence?.* [Em linha] Disponível em: http://www.nato.int/docu/review/2011/social_medias/cyber-defense-social-media/EN/ [Consult. em 24 mar. 2015].

Garside, D., Ponnusamy, A., Chan, S. & Picking, R., 2012. *Secure Military Social Networking and Rapid Sensemaking in Domain Specific Concept Systems: Research Issues and Future Solutions.* [Em linha] Disponível em: www.mdpi.com/1999-5903/4/1/253/pdf [Consult. em 20 mar. 2015].

George Patterson Y&R, 2011. *Review of Social Media and Defence.* s.l.:Australian Government: Department od Defence.

Governo de Portugal, 2013. *Conceito Estratégico de Defesa Nacional.* [Em linha] Disponível em: http://www.defesa.pt/Documents/20130405_CM_CEDN.pdf [Consult. em 31 mar. 2015].

GrupoMarktest, 2014. *Os Portugueses e as Redes Sociais 2014.* [Em linha] Disponível em: http://www.marktest.com/wap/private/images/logos/Folheto_redes_sociais 2014.pdf [Consult. em 22 mar. 2015].

GrupoMarktest, s.d. *Bareme Internet.* [Em linha] Disponível em: http://www.marktest.com/wap/a/grp/p~40.aspx [Consult. em 8 abr. 2015].

IESM, 2014a. *NEP/ ACA-010 Trabalhos de Investigação.* Lisboa: IESM.

IESM, 2014b. *NEP / ACA-018 Regras de Apresentação e Referenciação para os trabalhos escritos a realizar no IESM.* Lisboa: IESM.

inboundware.com, 2012. *Facebook: taxa de penetração em Portugal é de 83,4%.* [Em linha] Disponível em: http://www.inboundware.pt/taxa-de-penetracao-do-facebook-em-portugal/ [Consult. em 26 mar. 2015].

Internet Engineering Task Force, 1989. *RFC 1122: Requirements for Internet Hosts -- Communication Layers.* [Em linha] Disponível em: https://www.ietf.org/rfc/rfc1122.txt [Consult. em 4 abr. 2015].

Internet Engineering Task Force, 1994. *RFC 1738: Uniform Resource Locators (URL).* [Em linha] Disponível em: https://www.ietf.org/rfc/rfc1738.txt [Consult. em 17 abr. 2015].

Lisko, T., 2010. *The Robin Sage Experiment: Interview with Omachonu Ogali.* [Em linha] Disponível em: http://www.privacywonk.net/2010/09/the-robin-sage-experiment-interview-with-ogali-om.php [Consult. em 24 mar. 2015].

McCarthy, L., Watson, K. & Weldon-Siviy, D., s.d. *Own Your Space: A Guide to Facebook Security For Young Adults, Parents, and Educators.* [Em linha] Disponível em: https://www.facebook.com/safety/attachment/Guide%20to%20Facebook-%20Security.pdf [Consult. em 8 abr. 2015].

Mineiro, M. P., 2015. *A experiência da Força Aérea portuguesa relativa à utilização das redes sociais* [Entrevista] (Estado-Maior da FAP, 27 mar. 2015).

Ministério da Defesa Nacional, 1999. *Estatuto dos Militares das Forças Armadas (Decreto-Lei n.º 236/99, de 25 de junho).* Lisboa: Diário da República.

Ministério da Defesa Nacional, 2012. *Anuário Estatístico da Defesa Nacional.* Lisboa: Ministério da Defesa Nacional.

Mislove, A. E., 2009. *Em linha Social Networks: Measurement, Analysis, and Applications to Distributed Information Systems.* Houston: Rice University.

Moe, M. T. A., 2011. *Social Media and the U.S. Army: Maintaining a Balance.* Kansas: School of Advanced Military Studies.

Olston, C. & Najork, M., 2010. *Web Crawling.* [Em linha] Disponível em: http://infolab.stanford.edu/~olston/publications/crawling_survey.pdf [Consult. em 1 abr. 2015].

OTAN, 2009. *AJP-3.1O -Allied Joint Doctrine for Information Operations.* s.l.:Organização do Tratado do Atlântico Norte.

Parr, B., 2010. *The New MySpace: Screenshots and Videos.* [Em linha] Disponível em: http://mashable.com/2010/10/26/new-myspace/ [Consult. em 5 abr. 2015].

Ryan, T., 2010. *Getting In Bed With Robin Sage.* [Em linha] Disponível em: http://media.blackhat.com/bh-us-10/whitepapers/Ryan/BlackHat-USA-2010-Ryan-Getting-In-Bed-With-Robin-Sage-v1.0.pdf [Consult. em 24 mar. 2015].

Safko, L., 2012. *The Social Media Bible: Tactics, Tools, and Strategies for Business Success.* 3rd ed. New Jersey: John Wiley & Sons.

Santos, C. T. B. d. et al., 2014. *Orientações Metodológicas para a Elaboração de Trabalhos de Investigação.* Lisboa: IESM.

U.S. Army, 2014. *The United States Army Media handbook.* [Em linha] Disponível em: http://www.slideshare.net/USArmySocialMedia/social-media-handbook32-38656179 [Consult. em 21 mar. 2015].

U.S.Army, s.d. *U.S. Army Social Media Registration Checklist.* [Em linha] Disponível em: http://usarmy.vo.llnwd.net/e2/rv5_downloads/socialmedia/RegistrationChecklist.pdf [Consult. em 26 03 2015].

W3C, 2015. *HTML & CSS.* [Em linha] Disponível em: http://www.w3.org/standards/webdesign/htmlcss [Consult. em 6 abr. 2015].

Warden, P., 2010. *How I got sued by Facebook.* [Em linha] Disponível em: http://petewarden.com/2010/04/05/how-i-got-sued-by-facebook/ [Consult. em 30 mar. 2015].

Anexo B – Princípios orientadores para a política de utilização das RS pelos militares da defesa

Princípios aplicáveis no uso organizacional

Todos os militares que tenham responsabilidades na gestão dos conteúdos publicados nas presenças oficiais das organizações da defesa nas RS, devem considerar que:

-quaisquer comentários efetuados nas RS a título oficial, estão limitados aos elementos militares expressamente autorizados para tal, e reconhecidos como competentes para o fazer através da sua nomeação para funções relacionadas com o domínio das Relações Públicas;

-quaisquer comunicações oficiais devem ser efetuadas apenas nos canais oficiais, e só em casos muito excecionais poderão ser utilizadas para comunicar contas ou perfis pessoais, mas nesse caso obrigando a destacar a identidade do autor e a efetuar menção de que é um funcionário da organização devidamente autorizado para efetuar tal comunicação;

-quaisquer comentários devem incidir apenas em informações não-classificadas, e que ainda assim sejam consideradas adequadas para serem do domínio público;

-qualquer comunicação deve conter apenas informação fidedigna, relevante e cumpridora das políticas de comunicação em vigor na defesa;

-quem efetua uma comunicação deve estar inteiramente seguro que não está a efetuar nenhum anúncio em primeira mão, já que, se tal for o caso só poderá fazê-lo se possuir uma autorização específica;

-quaisquer comentários devem ser feitos apenas nas áreas de responsabilidade e de conhecimento do seu autor;

-quaisquer comentários devem ser feitos apenas quando exista uma garantia de que são respeitosos para com a comunidade a que se destinam;

-só poderão ser utilizados canais de comunicação em que seja possível garantir o total respeito pelos termos e condições de utilização impostos pelos mesmos, bem como o cumprimento total da legislação aplicável seja em termos de direitos de propriedade ou de privacidade, em linha com o definido nas políticas de comunicação em vigor;

-nunca devem, publicar ou comentar em resposta a comunicações que contenham informação e carácter ofensivo, obsceno, difamatório, ameaçador, assediador, intimidatório, discriminatório, odioso, racista, sexista, ou atentatório da lei ou da ética;

-nunca devem utilizar ou revelar qualquer informação classificada ou sensível;

-nunca devem fazer quaisquer comentários ou publicar quaisquer conteúdos que prejudiquem a imagem ou reputação da defesa(George Patterson Y&R, 2011, pp. 186-7).

Princípios aplicáveis no uso particular

Para orientar os militares enquanto utilizadores da RS na sua vida particular:

-devem ser criadas umas normas de conduta para a utilização das RS, contendo um conjunto de boas práticas;

-não deve ser restringido o uso das RS, mas sim, incentivado um comportamento respeitador das boas práticas;

-deve ser disponibilizada uma área de Perguntas Efetuadas Frequentemente;

-devem ser fornecidos exemplos de comunicações corretas e incorretas para facilitar a compreensão dos utilizadores;

-deve ser clarificada uma fronteira entre o uso privado aceitável e o não aceitável;

-devem ser transmitidas todas as instruções relativas à segurança da informação, à confidencialidade e à privacidade previstas pelas políticas da defesa em vigor;

-devem ser referidas quaisquer as diretivas ou normas de execução permanentes que possam estar relacionadas com a utilização da RS.

Todos os militares que trabalhem em organizações da defesa e utilizem as RS, devem ser educados para entender que:

-são responsáveis por tudo o que publicam nas RS;

-devem publicar ou comentar apenas informação que já seja do domínio público;

-devem garantir que todo o conteúdo publicado é fidedigno, não é enganador e que está em linha com as políticas em vigor na defesa;

-devem declarar expressamente naquilo que publicam quando estão identificados como membros da defesa que a opinião emitida é a sua pessoal e não a da defesa;

-podem incluir nas suas páginas a ressalva ou aviso legal que se sugere “As opiniões aqui expressas são opiniões pessoais e não refletem as opiniões da defesa”;

-devem ser educados e respeitosos para com as pessoas com quem se relacionam;

-devem aceitar e respeitar os termos de uso dos sítios ou plataformas das RS, bem cumprir totalmente a legislação aplicável seja em termos de direitos de propriedade ou de privacidade;

-não devem publicar conteúdos de carácter ofensivo, obsceno, difamatório, ameaçador, assediador, intimidatório, discriminatório, odioso, racista, sexista, ou atentatório da lei ou da ética;

-não devem aparentar que estão autorizados a falar como representantes da defesa, ou dar a ideia de que as opiniões expressas por si são as mesmas da defesa;

-não devem utilizar o seu endereço de correio eletrónico da defesa ou das suas organizações, bem como apresentar quaisquer logotipos ou insígnias ligados à defesa;

-não devem usar a identidade de qualquer outro membro ou entidade ligada à defesa;

-não devem divulgar nenhuma informação confidencial ou informação pessoal que tenham obtido nas suas funções na defesa;

-não devem publicar ou comentar sobre qualquer conteúdo que possa afetar a reputação ou denegrir a imagem da defesa (George Patterson Y&R, 2011, pp. 187-8).

Anexo C – Processo interno do *Department of Defense* dos EUA para revisão da informação a publicar nas RS

Para determinar se a informação pode ser libertada e qual a extensão dessa divulgação, a revisão terá sempre de ter em conta os princípios da Segurança da Informação, da Segurança das Operações, consistência da informação com outras disseminadas anteriormente, etc. A Figura 20 apresenta um fluxograma orientador dos procedimentos do processo que consta na diretiva DoDI 8550.01 de setembro de 2012.

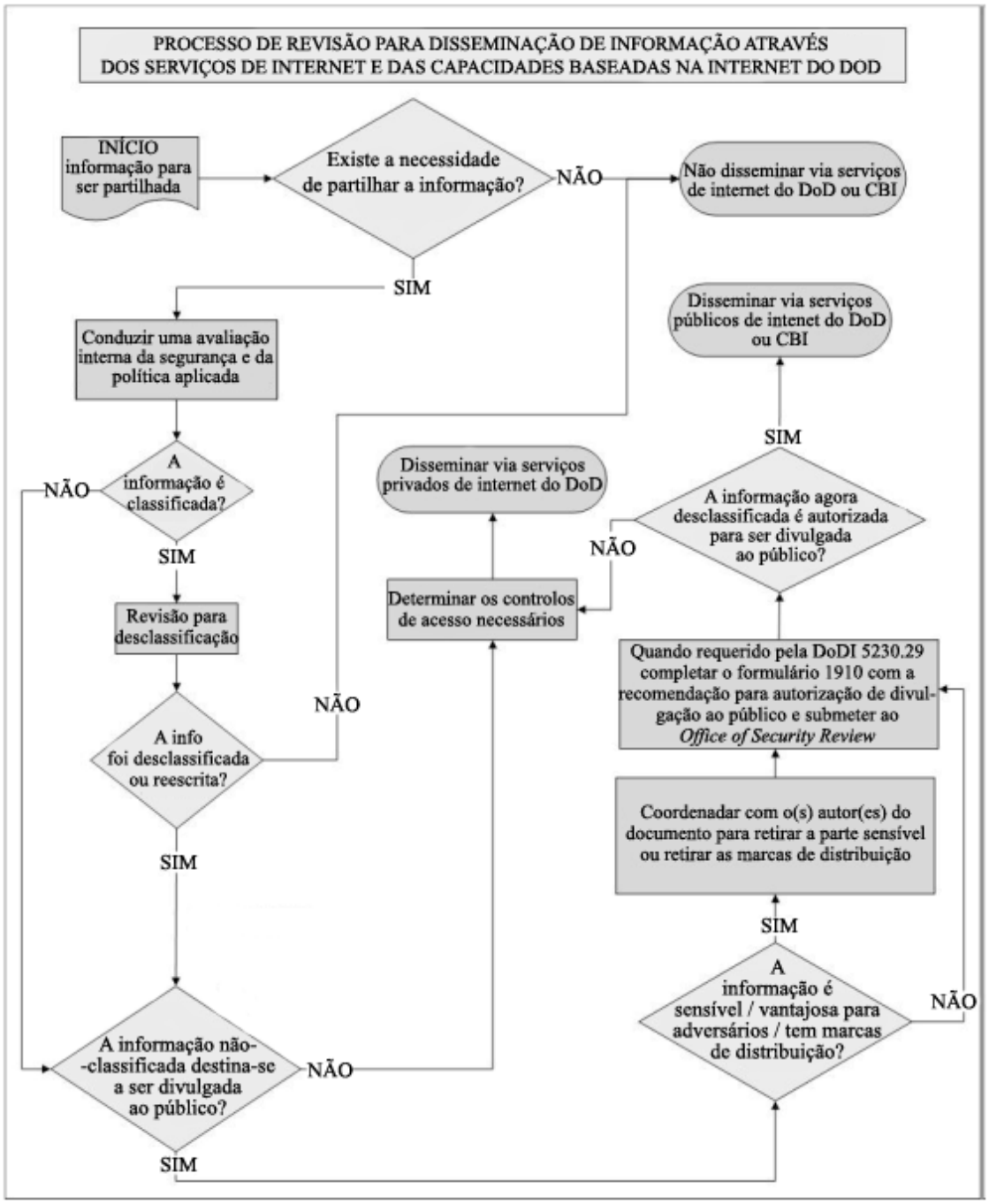

Figura 20 - Fluxograma do processo interno de revisão da informação do *DoD*
Fonte: (Department of Defence, 2012, p. 39)

Anexo D – Técnicas recomendadas pelo Exército dos EUA para a construção de páginas no Facebook

O Exército dos EUA disponibiliza o documento "U.S. Army Social Media Handbook 3.2" na plataforma *Slideshare*, contendo um guia com as técnicas recomendadas para a construção de páginas no Facebook, tendo estas sido extraídas de uma seleção de páginas existentes nesta RS que foram escolhidas por serem consideradas as mais eficazes para uma comunicação organizacional. Assim o documento intitulado "Folha de referência rápida do Facebook" inclui o conjunto de técnicas que a seguir se apresenta. (U.S. Army, 2014, p. 24).

O que se deve fazer:

-Comece com uma estratégia bem definida – para tal é necessário responder à pergunta "como é que os *media* sociais se encaixam nos seus objetivos de comunicação?";

-Publique as suas mensagens ao longo do dia; não as publique todas em simultâneo;

-Publique à noite e aos fins-de-semana e avalie quais os períodos melhores;

-Referencie pelo menos outra página em cada publicação;

-Tente efetuar uma pergunta de envolvimento para cada publicação;

-Responda às perguntas em tempo oportuno;

-Faça publicações e siga e estimule uma política de comentários;

-Lembre-se de publicar num tom mais amigável, mas não profissional;

-Faça uma verificação ortográfica das suas publicações antes de as submeter;

-Agradeça aos seus seguidores e elogie-os muitas vezes;

-Use muitas fotografias de alta qualidade (não se esqueça de adicionar o máximo possível de detalhes sobre a mesma e de pedir ao seu público para também o fazer, como forma de o envolver, ou de lhes pedir para se referenciarem a si ou outrem nessa fotografia);

-Use vídeos curtos, não-editados e apelativos;

-Antes de publicar pergunte a si mesmo: "eu iria partilhar isto com meus amigos?";

-Misture diferentes elementos na página: fotografias, perguntas, vídeos, partilha de conteúdo de outros, notícias, etc.

-Dê um toque pessoal ao que publica para envolver o seu público;

-Incentive a participação, colaboração e feedback do público;

-Procure um URL[16] curto e inteligente para a página (facebook.com/username);

-Atualize as fotografias de perfil frequentemente (procure mostrar uma variedade de atividades, ângulos, pessoas, etc.);

-Peça a alguém ler as suas mensagens antes de as publicar;

-Acompanhe as estatísticas de acessos à página e avalie o interesse despertado pelos seus conteúdos. Determine métricas importantes antes de se envolver, defina um ponto de referência e acompanhe a sua *performance* ao longo do tempo;

-Faça "Gosto" nas organizações similares e referencie-as com frequência;

-Publique informações ou comentários noutras páginas utilizando o perfil da sua organização (não esquecendo que está a publicar como organização);

-Respeite sempre a OPSEC ao publicar;

-Procure identificar as entidades ou órgãos indicados para responder a perguntas que surjam na sua página, ou reenvie-lhes essas perguntas em busca da resposta para publicar;

-Pergunte aos seus seguidores o que eles gostariam de ver na página.

O que não se deve fazer:

-Não efetue publicações demasiadas vezes ao dia (irá perder seguidores);

-Não altere a ordem de todas as suas publicações ao mesmo tempo;

-Não tente demasiado vender ideias;

-Evite publicar mensagens clichê ou comunicados de imprensa aborrecidos, a não ser em último recurso;

-Não use linguagem própria dos adolescentes nas RS em publicações profissionais;

-Não utilize funcionalidades ou aplicações georreferenciadas na sua página (ex: a mostrar a localização onde está a publicar através do Twitter);

-Não publique uma hiperligação sem lhe dar algum título sugestivo ou descrição;

-Nunca remova o conteúdo de comentários deixados por outros só porque este não lhe agrada. Se ele não violar a política estabelecida para os comentários, deixe-o!

E lembre-se:

-Não controla uma mensagem a partir do momento em que esta é publicada;

-Um único deslize profissional pode ser o suficiente para manchar a sua reputação;

-Se não tiver disponibilidade para monitorizar a sua página, então restrinja os contributos dos outros (fotografias, vídeos, comentários, etc.).

[16] *Uniform Resource Locator* (URL) – sintaxe e semântica formal para a informação necessária para localizar um recurso na Internet (Internet Engineering Task Force, 1994).

Anexo E – Técnicas recomendadas pelo Exército dos EUA para a utilização do Twitter

O Exército dos EUA disponibiliza o documento "U.S. Army Social Media Handbook 3.2" na plataforma *Slideshare*, contendo um guia com as técnicas recomendadas para a utilização do Twitter, tendo estas sido escolhidas por serem consideradas as mais eficazes para uma comunicação organizacional. Assim o documento intitulado "Folha de referência rápida do Twitter" inclui o conjunto de técnicas que a seguir se apresenta. (U.S. Army, 2014, p. 25).

-Seja criativo e publique diferentes tipos de informação;

-use URL curtos;

-use *hashtags* em cada *tweet*, procurando alguns já existente e criando novos;

-*tweet* hiperligações para conteúdos (artigos, fotografias, sítios web);

-*tweet* as últimas notícias relacionadas com a sua unidade;

-*tweet* citações dos oficiais de alta patente com maior destaque;

-*tweet* eventos em direto;

-crie os seus próprios *hashtags* para eventos e publicite-os várias vezes desde cedo;

-use o Twitter para comunicar durante uma crise;

-siga as contas no Twitter das outras organizações da defesa;

-procure com frequência novas contas no Twitter, siga-as e partilhe os seus conteúdos;

-*retweet* conteúdos de outras contas acrescentando uma mensagem da sua organização;

-relacione-se com a sua audiência do Twitter colocando questões e *retweeting* as suas respostas

-inclua nomes de utilizador de outras contas nos seus *tweets* de modo a incrementar o reconhecimento e o seguimento;

-esteja atento ao que os seus seguidores estão a falar;

-pergunte a si mesmo "Eu iria querer fazer *retweet* do que estou prestes a fazer *tweet*?";

-verifique as suas mensagens diretas e menções diariamente e responda;

-crie uma voz e uma personalidade para a sua instituição;

-procure tornar-se o recurso preferido para obter notícias recentes e informação;

-utilize mensagens diretas para se envolver com os seguidores da sua organização;

-coloque o seu foco no conteúdo mais extraordinário existente no Twitter;

-Alterne os tempos de envio de *tweets*;

-edite os seus *tweets* e evite *typos*;

-inclua uma ressalva ou aviso legal (Seguir não significa concordância);

-associe a sua página à marca;

-inclua uma hiperligação para o seu sítio oficial na sua biografia;

-liste a sua página do Twitter na sua página do Facebook;

-use *twitpics*.

O que não se deve fazer:

-Não *tweet* demasiadas vezes ao dia (irá perder seguidores);

-não altere a ordem de todos os seus *tweets* ao mesmo tempo;

-não siga marcas (Coca-Cola, Pepsi, etc.) pode parecer seu representante;

-não siga impostores ou indivíduos com afiliações políticas ou religiosas;

-não se torne obsessivo com o número de seguidores que tem;

-não *tweet* à hora certa (toda a gente o faz);

-não seja demasiado promocional;

-não *tweet* com linguagem vulgar usada no Twitter (por exemplo “lol”);

-não deixe estagnar a sua conta (não fique mais de uma semana sem *tweetar*);

-não adicione localizações aos *tweets;*

-não conecte o Twitter ao Facebook.

E lembre-se:

-Não controla um *tweet* a partir do momento em que este é enviado;

-quando um *tweet* seguiu, ele anda por aí;

-se está a tweetar a partir de um dispositivo móvel, certifique-se que não mistura o profissional com o particular no mesmo dispositivo.

Anexo F – Dicas de segurança recomendadas pelo Facebook no seu Guia de Segurança

Da informação contida na publicação *Em linha* "A Guide to Facebook Security or Young Adults, Parents, and Educators", disponível no sítio do Facebook, ressalta-se "As Melhores Dicas para se manter seguro no Facebook" que constitui um lista de elementos úteis a divulgar em quaisquer normas de utilização e que a seguir se apresenta:

1º Estabeleça "Amizade" nas RS apenas com pessoas que você conhece.

2º Crie sempre palavras-chave fortes para aceder às suas contas ou perfis nas RS e use palavras-chave diferentes para cada.

3º Nunca divulgue as suas palavras-chave a outras pessoas.

4º Altere as suas palavras-chave regularmente.

5º Partilhe as suas informações pessoais apenas com pessoas ou empresas que necessitam realmente dessa informação.

6º Faça o *login* nos sítios das RS apenas uma vez por cada sessão. Se lhe parecer que a RS está a solicitar-lhe que efetue um segundo *login*, deve de encerrar o seu *browser* ou aplicação e abrir uma nova sessão, introduzindo diretamente o endereço do sítio na barra de endereços.

7º Altere a sua palavra-chave, logo após a utilizar no computador de outra pessoa.

8º Termine sempre a sua sessão depois de utilizar o computador de outra pessoa.

9º Use a navegação segura sempre que possível, identificável através da presença do prefixo *https* nos endereços.

10º Descarregue aplicativos apenas a partir de sítios confiáveis.

11º Mantenha o seu *software* anti-vírus atualizado.

12º Mantenha o seu *browser* ou outros aplicativos que utilize para aceder às RS atualizados.

13º Não faça cópia/colagem de código para a barra de endereços do seu *browser*.

14º Use os suplementos de segurança existentes para o seu *browser*, de modo a proteger a sua conta da possibilidade de ser sequestrada.

15º Tenha cuidado com mensagens "inesperadas" que procuram despertar a sua curiosidade para o conteúdo, mesmo que sejam provenientes de "Amigos".

16º Não se esqueça que os *hackers* se podem apoderar das contas dos seus amigos e a partir destas enviar-lhe *links*. Tenha cuidado com *links* sugestivos mesmo que sejam provenientes dos seus amigos (McCarthy, et al., s.d., p. 13).

Apêndice A – Modelo de análise

Nas tabelas 10, 11 e 12 encontram-se definidos os conceitos, dimensões, indicadores que gerarão informação no sentido de avaliar as hipóteses previamente levantadas.

Tabela 3 - Conceitos, Dimensões e Indicadores associados à Hipótese 1
Fonte: autor, 2015

QD1: Como são hoje as RS e qual a relação dos portugueses com estas enquanto seus utilizadores particulares ou profissionais?		
H1: As RS são um fenómeno em contínuo crescimento, com características distintas em termos geográficos e dinâmicas imprevisíveis, e são para os portugueses que acedem regularmente à Internet algo indispensável.		
Conceitos	Dimensões	Indicadores
C1 - Rede Social	D1.1 - Física	I1.1.1- Tecnologia I1.1.2 -Software I1.1.3 -Dispositivos I1.1.4 -Conteúdos
	D1.2 - Social	I1.2.1 -Relações I1.2.2 -Partilha I1.2.3 -Horários

Tabela 4 - Conceitos, Dimensões e Indicadores associados à Hipótese 2
Fonte: autor, 2015

QD2: A especificidade das atividades desenvolvidas pela defesa impede o uso das RS nos seus ambientes de trabalho?		
H2: A tecnologia está cada vez mais presente nos ambientes de trabalho da defesa e o uso das RS em simultâneo nestes ambientes aumenta fortemente a ameaça à segurança da informação e à segurança das operações.		
Conceitos	Dimensões	Indicadores
C1 – Elementos militares	D1.1 - Profissional	I1.2.1 - Forma de Prestação de serviço I1.2.1 – Funções atribuidas
C2 - Regulamento de Disciplina Militar	D2.1 - Comportamental	I2.1.1 - Linguagem desadequada I2.1.2 - Ideias contrárias à constituição e leis da república I2.1.3 - Partidarismo político
	D2.2 - Ético	I2.2.1 - Revelação de matérias sensíveis ou confidenciais I2.2.2 - Indisciplina
C3 - Segurança da Informação	D3.1 - Pessoal	I3.1.1 - Divulgação intencional I3.1.2 - Divulgação negligente

Tabela 5 - Conceitos, Dimensões e Indicadores associados à Hipótese 3
Fonte: autor, 2015

QD3: É possível criar regras que minimizem as ameaças e tornem aceitável o uso simultâneo das RS por elementos militares?		
H3: É necessário criar normas de conduta para os militares que utilizam as redes sociais e as semelhanças existentes nas diversas estruturas das FFAA aconselham a definição de uma política comum.		
Conceitos	Dimensões	Indicadores
C1 – Política Comum	D1.1 - Acesso	I1.1.1 – Conteúdos I1.1.2 – Dispositivos I1.1.3 – Horários
	D1.2 - Monotorização	I1.2.1 – Objeto I1.2.2 – Técnicas I1.2.3 – Agentes
	D1.3 - Formação	I1.3.1 – Objeto I1.3.2 - Agentes
C2 - Normas de Conduta	D2.1 - Aplicabilidade	I2.1.1 - Destinatários I2.1.2 - Contexto
C3 - Rede Interna	D3.1 - Utilidade	I3.1.1 - Conteúdos I3.1.2 - Aplicabilidade

Apêndice B – Guião da entrevista realizada ao Chefe da Área de Informação Pública da Força Aérea Portuguesa em 27/3/2015

O Gabinete de Relações Públicas da Força Aérea portuguesa, na pessoa do Sr. Major Paulo Mineiro, Chefe da Área da informação Pública, aceitou gentilmente responder em entrevista a um conjunto de perguntas subordinadas ao tema "A experiência da Força Aérea portuguesa relativa à utilização das redes sociais". Esta entrevista realizou-se no dia 27 de Março de 2015 nas instalações do Estado-Maior da FA e seguiu o guião que a seguir se apresenta (Mineiro, 2015).

Parte I - Presença Organizacional

1º Qual foi o momento e quais foram as razões para a decisão da criação das presenças da Força Aérea nas redes sociais?

2º Foi feito algum plano para este processo de entrada nas RS?

3º Quais julga terem sido os objetivos delineados nessa altura?

4º Foram estes objetivos foram alcançados à data de hoje? Sofreram alterações desde o início?

5º Da experiência adquirida quais são as principais vantagens e as desvantagens da utilização das RS pela FA?

6º De que forma mede o retorno desta participação?

7º Existe forma de diferenciar o retorno, medido por exemplo em nº de seguidores: os que já são militares da FA, os que são seus familiares ou os que são militares doutros ramos das FFAA?

Parte II - Presença Pessoal

8º Existe alguma preocupação com a utilização pessoal das RS por parte dos militares da FA ou de outras presenças de entidades subordinadas à FA?

9º Existe uma política definida para a utilização nos ambientes de trabalho da FA?

10º Existe ou é possível vir a existir normas de conduta para a utilização das redes sociais?

11º Como visualiza a monotorização dos perfis públicos dos militares ou entidades subordinadas à FA?

Muito obrigado.